A. PROPUESTA PROYECTO DE INVESTIGACIÓN

1. TIPO DE PROYECTO:

Interno	**X**	**Grupal**	
Semilla		**Multidisciplinario**	

2. TIPO DE INVESTIGACIÓN:

Básica		**Aplicada**	**X**

3. UNIDAD EJECUTORA *(Departamento, Instituto o Estructura de Investigación):*

1. Departamento de Electrónica, Telecomunicaciones y Redes de Información.

4. LINEA(S) DE INVESTIGACIÓN:

1. Privacidad y seguridad Seguridad y privacidad

5. TÍTULO DEL PROYECTO *(mínimo 10 palabras):*

Soporte a la experimentación en el diseño de sistemas respetuosos con la privacidad

6. RESUMEN *(máximo 200 palabras)*

En el mundo digital actual, los datos se han convertido en un recurso extremadamente preciado que mantiene el modelo de negocio de varias organizaciones. A la vez, la explotación de los datos personales tienen implicaciones fuertes en la privacidad. Por ejemplo, mucha gente ha quedado expuesta ante filtraciones masivas de sus datos. Uno de los mecanismos de protección, es el diseñar los sistemas con consideraciones de privacidad desde el inicio. Métodos, técnicas y herramientas son investigadas para ayudar a los desarrolladores en el proceso de diseño. Sin embargo, la mayoría de ellas han quedado en un nivel filosófico o de solución, faltando una validación empírica para probar su utilidad o beneficios.

Con el fin de contribuir a solventar esta carencia, este proyecto da un paso fundamental y proveerá un conjunto de instrumentos (en forma de taxonomías, clasificaciones, etc.) y una herramienta de soporte que pueden ser usados para diseñar y llevar a cabo experimentos para validar los métodos de diseño respetuosos con la privacidad. Nos enfocamos en aquellos basados en estrategias y patrones. Esto debido a que han captado mayoritariamente la atención de los investigadores e incluso han llegado a formar parte de recomendaciones de agencias de ciberseguridad internacionales.

7. PALABRAS CLAVE *(4-6)*

Ingeniería de privacidad, privacidad desde el diseño, patrones de privacidad, experimentación

8. OBJETIVOS

8.1. OBJETIVO GENERAL

Generar instrumentos para la experimentación con métodos de diseño de sistemas respetuosos con la privacidad basados en estrategias y patrones.

8.2. OBJETIVOS ESPECÍFICOS

a. Analizar los métodos de diseño de sistemas respetuosos con la privacidad basados en estrategias y patrones, y el proceso de experimentación aplicado a ellos.
b. Generar un conjunto de instrumentos reusables para llevar a cabo experimentos con el tipo de métodos previamente analizados.
c. Desarrollar una herramienta que brinde soporte a la experimentación con el tipo de métodos analizados en este proyecto.
d. Validar el soporte a la experimentación provisto a través de una prueba de concepto.
e. Divulgar los resultados y la temática investigada.

9. HIPÓTESIS (opcional)

N/A.

10. DETALLE DE LOS RESULTADOS ESPERADOS *(con relación a los objetivos)*

a. Informe sobre el análisis de los métodos de diseño de sistemas respetuosos con la privacidad que están basados en estrategias y patrones, y sobre el proceso de experimentación con ellos. El análisis tendrá en cuenta instrumentos necesarios para experimentar como: el tipo de problema o escenario de referencia de diseño con requisitos de privacidad, el tipo de objeto que se podría estudiar (p.ej. una solución a un problema de diseño), el efecto que se podría evaluar (p.ej. la completitud de una solución de diseño), las métricas que se podrían usar para determinar el efecto estudiado (p.ej. número de requisitos cumplidos, número de patrones escogido), y otros instrumentos propios de los métodos de diseño estudiados (p.ej. guías para aplicar estrategias de diseño, taxonomías de estrategias, catálogos de patrones).
b. Un conjunto de instrumentos reusables para la experimentación con el tipo de métodos estudiados. Este conjunto estará compuesto por taxonomías o clasificaciones de los instrumentos requeridos, y actuará como una caja de herramientas que facilite la creación de experimentos en el contexto de los métodos de diseño estudiados o similares.
c. Una herramienta de software que brinde soporte a la experimentación con métodos de diseño basados en estrategias y patrones y donde se haga uso de los instrumentos previamente creados.
d. Un trabajo de titulación de pregrado donde se desarrolle la herramienta de software.
e. Un reporte de una prueba de concepto. Esta prueba incluye el diseño de un experimento, haciendo uso de los instrumentos establecidos, y las pruebas de validación de la herramienta soportando el diseño definido.
f. El envío de un artículo o presentación en congreso (indexados en Scopus, Scielo o WoS) reportando los resultados científicos alcanzados.
g. La presentación de la temática, su necesidad e importancia y de los resultados alcanzados a través de charlas abiertas.

11. IMPACTO DE LA INVESTIGACIÓN (*científico, social, económico u otros*)

Este proyecto de investigación contribuye al área del diseño de sistemas respetuosos con la privacidad de las personas. Esta provee métodos, técnicas y herramientas para el diseño de sistemas de información que respetan la privacidad de las personas, que son requeridos por las organizaciones que brindan servicios basados en datos y que deben estar alineadas con las legislaciones pertinentes. En tal sentido, el impacto de este proyecto de investigación es:

- a nivel de las personas, proveyendo y validando mecanismos para proteger el derecho a la privacidad,
- a nivel económico, al proporcionar mecanismos validados para que las organizaciones puedan cumplir con las legislaciones y así continuar con sus modelos de negocio basados en datos,
- a nivel de ingeniería, brindadando medios a los ingenieros y desarrolladores para diseñar sistemas,
- a nivel científico, con el avance y validación de los medios en el área del diseño de sistemas respetuosos con la privacidad, con la conformación de nuevas líneas de investigación y con la colaboración con investigadores internacionales, y
- a nivel docente, con la impartición de charlas magistrales en asignaturas de pregrado y posgrado.

El **impacto a la protección a la privacidad** [1] **de las personas** incluye: la privacidad de los datos personales, de las comunicaciones, del comportamiento, de la localización, etc. (Clarke, 1997) (Finn, Wright y Friedewald, 2013). Asimismo, el impacto en la protección de la privacidad de las personas puede ser abordado desde diferentes (Clarke, 1997): psicológico, ya que las personas necesitan un espacio privado para pensar; sociológico, ya que las personas necesitan comportarse en grupo sin temor a monitorizaciones; político, ya que limitaciones a la privacidad de comportamiento o injerencias en él pueden amenazar la democracia; entre otros.

Esta investigación aporta específicamente a la implementación de la protección de datos (y de la privacidad) desde el diseño mandada en aquellas legislaciones de protección de datos personales basadas en el Reglamento General de Protección de Datos Europeo (European Parliament & Council of the European Union, 2016). Una de las cuales es la Ley de Protección de Datos Personales del Ecuador, que se encuentra actualmente en la Asamblea Nacional (Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador, 2019) (La revista, 2020) (Asamblea Nacional del Ecuador, 2019), y que es parte fundamental del programa de acción "Ecuador eficiente y ciberseguro" del plan "Ecuador digital". La alineación a estas legislaciones permite, además de proteger la privacidad de las personas, la adecuada explotación de los datos personales a través de diferentes modelos de negocio. Se tiene así un **impacto a nivel económico**.

El cumplimiento de las legislaciones locales y regionales (en especial de aquellos socios económicos como la Unión Europea) posibilita cumplir con los requerimientos para acceder al mercado global de datos y servicios que se está creando. Acorde a las Naciones Unidas [2], 132 países ya disponen de una legislación de protección de datos y privacidad, y la europea es una de las más desarrolladas. En este contexto, las organizaciones deben implementar medidas técnicas y organizativas para la protección de datos.

Este trabajo contribuye, desde la perspectiva técnica, a generar y validar los medios que los ingenieros necesitan para diseñar sistemas respetuosos con la privacidad a usarse en las organizaciones. De este modo, **se impacta el proceso de ingeniería**. Diseñar sistemas respetuosos con la privacidad de las personas no es una tarea trivial, y por ello los ingenieros necesitan herramientas, técnicas y métodos que les ayuden en el proceso de diseño. Estos mecanismos pueden acoplarse a los procesos de trabajo que siguen los desarrolladores, facilitar la comprensión de los conceptos de privacidad, hacer más eficientes los procesos, ayudar a generar diseños de mejor calidad, etc.

El estado del arte en esta área de investigación reporta varias propuestas de soluciones, pero aún se requiere validarlas o evaluarlas. Este proyecto de investigación busca crear los instrumentos necesarios y fundamentales para, posteriormente, llevar a cabo las validaciones y evaluaciones de aquellas propuestas de métodos o procesos basados en estrategias y patrones. Se genera así, **un impacto a nivel científico**.

[1] La privacidad, según la Real Academia Española, es "el ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión".

[2] https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

Otros aportes a nivel científico de este proyecto investigación incluyen: el brindar sustento para consolidar la línea de investigación en análisis y diseño de sistemas de tecnologías de información respetuosos con la privacidad, el colaborar con investigadores internacionales en esta área emergente y relevante a nivel global, y el realizar publicaciones científicas de alto impacto. Debido a que es un área nueva y relevante a nivel global, y considerando la experiencia previa de los investigadores, es una oportunidad para consolidar las líneas de investigación en el ámbito de la ingeniería de privacidad.

Finalmente, es una oportunidad para generar y transmitir conocimiento de actualidad a los estudiantes de pregrado y posgrado a través de sesiones en asignaturas pertinentes y de charlas magistrales abiertas. De este modo, **se impacta en la docencia**.

12. ESTADO DEL ARTE, E INVESTIGACIONES PREVIAS DEL EQUIPO *(máximo tres carillas)*

Estado del arte

En el mundo digital actual, los datos personales han llegado a convertirse en el nuevo petróleo de Internet (Kuneva, 2009) y son parte fundamental de un escenario complejo. Por un lado, las personas están cada vez más preocupadas por su privacidad (TNS Political & Social, 2016), y por otro, los datos personales son la materia prima usada por las organizaciones para proveer productos y servicios. Además, cada vez hay más escándalos por el uso masivo e ilícito de datos. Por ejemplo, el caso de Facebook y Cambridge Analytica (Cadwalladr & Graham-Harrison, 2018) o la filtración de datos personales de millones de ciudadanos ecuatorianos[3].

En este escenario, han surgido legislaciones para proteger los datos personales (y la privacidad de las personas) y para generar confianza de modo que se pueda aprovechar todo el poder de los datos por parte de las organizaciones. Estas legislaciones (incluyendo el caso ecuatoriano con la Ley de Protección de Datos Personales del Ecuador (Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador, 2019) contemplan dentro de sus artículos la protección de datos personales desde el diseño de los sistemas. Este concepto se refiere a implementar medidas que protejan los datos personales (y la privacidad) de los individuos desde las etapas iniciales del proceso de creación de los sistemas que usan datos personales.

Estudios recientes del estado del arte (Caiza et al., 2019) (Morales-Trujillo et al., 2019) reportan que la cantidad de contribuciones para el diseño de sistemas respetuosos con la privacidad va en aumento. Las propuestas incluyen elementos como métodos, modelos, técnicas y herramientas, mismas que son indispensables de cara a brindar soporte a los desarrolladores en el proceso de diseño de los sistemas respetuosos con la privacidad.

Las contribuciones en torno a los patrones de privacidad[4] son las que han recibido mayor atención. En (Caiza et al., 2019), hay 28 artículos primarios de 66 estudiados que reportan avances en torno a los patrones. Asimismo, en (Morales-Trujillo et al., 2019), 12 de los 37 artículos primarios corresponden a los patrones. Incluso, en (Lenhard, Fritsch & Herold, 2017) realizan un estudio exclusivo sobre los patrones de privacidad, considerando 49 artículos. Este gran interés en investigar sobre patrones de privacidad podría deberse a algunas características de los patrones como: el organizar el conocimiento existente generalmente de expertos, el estar orientados a su uso por desarrolladores no expertos (en nuestro caso, en el ámbito de la privacidad), el ser un concepto ampliamente conocido por los desarrolladores y diseñadores de software, el considerar contexto con diferentes fuerzas (en el caso de la privacidad implicaciones técnicas, legales, personales, etc.) entre otras.

Dos tendencias se han encontrado en torno a las contribuciones basadas en patrones de privacidad: aquellas que desarrollan nuevos patrones y que los evolucionan hacia conjuntos más

[3] https://www.vpnmentor.com/blog/report-ecuador-leak/
[4] Basados en el concepto de patrón, que es usado en varios dominios de conocimiento, es una solución a un problema que se repiten en entornos determinados.

cohesivos e interrelacionados y aquellas que las incluyen dentro de sus procesos. Al primer grupo pertenecen propuestas como las de (Schumacher, 2003) (Sadicoff, Larrondo-Petrie & Fernández, 2005) (Romanosky et al., 2006) que presentan patrones individuales, los catálogos que reúnen patrones categorizados bajo esquemas comunes (Notario et al., 2015) (Drozd, 2016) (Chung et al., 2004) (Fischer-Hübner et al., 2010), los sistemas con patrones fuertemente interrelacionados (Colesky et al., 2018) (Colesky & Caiza, 2019) y los lenguajes de patrones más cohesivos y para dominios específicos (Shümmer, 2004) (Hafiz, 2013). Al segundo grupo pertenecen propuestas de métodos (Kalloniatis, Kavakli, & Gritzalis, 2008) (Kung, 2014) (Hoepman, 2014) y herramientas (Drozd, 2016) (Pearson & Shen, 2010) (Pearson & Benameur, 2011).

A pesar de tener una cantidad creciente de contribuciones, aún se requieren aquellas que validen o evalúen las propuestas existentes para ir más allá de propuestas filosóficas y soluciones argumentadas (Lenhard, Fritsch & Herold, 2017) (Caiza et al., 2019). Usualmente las propuestas de métodos que incluyen patrones de privacidad, no han realizado validaciones o evaluaciones, sino únicamente argumentaciones asumiendo que los patrones de privacidad están listos para aplicar (Caiza et al., 2019) y extrapolando los beneficios de otros dominios como el de la orientación a objetos (Gamma et al., 1995).

Es indispensable la validación y evaluación de estos métodos para demostrar los beneficios y utilidad de estas propuestas de cara a fomentar su adopción. Sin embargo, dada la necesidad urgente de brindar soporte a los desarrolladores e ingenieros para cumplir con las legislaciones, algunas propuestas como el enfoque basado en estrategias de diseño (Hoepman, 2014) ya forma parte de reportes y recomendaciones técnicas realizadas por la Agencia Española de Protección de Datos (Agencia Española de Protección de Datos, 2019) y la Agencia de la Unión Europea para la Ciberseguridad (Danezis et al., 2014).

En este escenario, se requieren contribuciones que validen y evalúen empíricamente aquellas propuestas basadas en estrategias de diseño y en patrones de privacidad. Esto brindará evidencia para cuantificar los beneficios y utilidad de las propuestas existentes. Este proyecto de investigación contribuye en esta línea, y se enfoca en reunir y construir los instrumentos necesarios para realizar experimentos futuros de una manera más versátil y rápida.

El área a explorar va en línea con nuestras investigaciones y conocimiento previo: diseño con requisito de privacidad usando patrones, y se concentra en una línea relevante y urgente como es la validación y evaluación empírica de las propuestas existentes.

Publicaciones de investigaciones previas relacionadas

Publicaciones previas en revistas de alto impacto (JCR Q1 e indexadas en Scopus)

- Guaman, D. S., Del Alamo, J. M., & Caiza, J. C. (2020). A Systematic Mapping Study on Software Quality Control Techniques for Assessing Privacy in Information Systems. IEEE Access, 8, 74808–74833. https://doi.org/10.1109/access.2020.2988408
- 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

Publicaciones previas en congresos internacionales de relevancia (Ranking CORE[5] e indexadas en Scopus)

- Caiza, J. C., Del Alamo, J. M., & Guamán, D. S. (2020). A framework and roadmap for enhancing the application of privacy design patterns. The 35th ACM/SIGAPP Symposium On Applied Computing, 1297–1304. https://doi.org/10.1145/3341105.3375768
- 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

[5] Ranking de conferencias internacionales http://portal.core.edu.au/conf-ranks/

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
- Del Alamo, J. M., Martín, Y. S., & Caiza, J. C. (2018). Towards organizing the growing knowledge on privacy engineering. In IFIP Advances in Information and Communication Technology (Vol. 526, pp. 15–24). https://doi.org/10.1007/978-3-319-92925-5_2
- Caiza, J. C., Martín, Y.-S., Del Alamo, J. M., & Guamán, D. S. (2017). Organizing design patterns for privacy: A taxonomy of types of relationships. Proceedings of the 22nd European Conference on Pattern Languages of Programs - EuroPLoP '17, 1–11. https://doi.org/10.1145/3147704.3147739
- Argudo, A., López, G., & Sánchez, F. (2017). Privacy vulnerability analysis for Android Applications: A practical approach. In 2017 Fourth International Conference on eDemocracy & eGovernment (ICEDEG) (pp. 256-260). IEEE.
- Lopez, G., Richardson, N., & Carvajal, J. (2015). Methodology for data loss prevention technology evaluation for protecting sensitive information. Revista Politécnica, 36(3), 69.

Proyectos de investigación relacionados con los cuales se han realizado trabajos conjuntos

PDP4E (2018 - 2021): Methods and tools for GDPR (General Data Protection Regulation) compliance through Privacy and Data Protection Engineering (Acuerdo No. 787034). Programa de investigación e innovación Horizonte 2020 de la Unión Europea. Este proyecto busca proporcionar a los ingenieros con métodos y herramientas para la creación de sistemas que cumplan con el RGPD, en particular en lo referente a la privacidad y protección de datos desde el diseño.

Se colaboró con el equipo de la Universidad Politécnica de Madrid en la revisión y análisis del estado del arte de los elementos de diseño (p.ej. métodos, modelos, herramientas). El resultado ha sido publicado en uno de los artículos de revista de alto impacto previamente citados.

P4P (2014 - 2018): Patterns for Privacy. Agenda de Investigación de Ciberseguridad Nacional por la Organización de los Países Bajos para la Investigación Científica (NWO/STW National Cyber Security Research Agenda –NCSRA II– programme). Este proyecto buscaba proveer a los diseñadores de sistemas un conjunto de herramientas que puedan aplicarlas en el diseño respetuoso con la privacidad. Principalmente se enfocaban en definir un catálogo extenso de patrones y herramientas basadas en los patrones para soportar el proceso de desarrollo de los sistemas.

Se colaboró con investigadores de ese proyecto para conseguir la evolución del catálogo de patrones hacia dos sistemas de patrones de privacidad reportados en los artículos previamente listados.

Privacy patterns (privacypatterns.org). Es un proyecto abierto y en marcha con investigadores de varias universidades internacionales: Clever, Escuela Politécnica Nacional, Inria, Radboud University, UC Berkeley School of Information, Ulm University, Universidad Politécnica de Madrid, Vienna University of Economics and Business.

Aquí se han implementado varias de las contribuciones realizadas previamente y reportadas en los artículos listados.

13. DESCRIPCIÓN DETALLADA DEL PROYECTO, INCLUIDO METODOLOGÍA *(máximo tres carillas)*

Este proyecto de investigación contribuye a la línea de provisión de evidencia empírica sobre de métodos de diseño con requisitos de privacidad basados en estrategias de diseño y patrones. Provee un conjunto fundamental de instrumentos que puedan ser usados al diseñar experimentos para validar y evaluar este tipo de métodos. Los instrumentos actuarán como una caja de herramientas que facilita el diseño y puesta en marcha de futuros proyectos de experimentación en el dominio.

La estrategia general a usarse estará basada en la búsqueda de información siguiendo un proceso sistematizado, usando como guía los pasos de estudios sistemáticos de literatura (Petersen, Vakkalanka & Kuzniarz, 2015) y la teoría fundamentada (Glaser & Strauss, 2017) para construcción de conocimiento. Estas estrategias serán adoptadas debido a la existencia de áreas de investigación próximas y más maduras como los patrones de seguridad y los patrones de diseño. Por un lado, estas áreas tienen un amplio estado del arte en temas de utilidad para el presente proyecto de investigación, por lo que se requiere realizar un proceso de búsqueda ordenado y sistematizado. Por otro lado, el análisis en profundidad de los trabajos relevantes (sus similitudes, características, etc.) permitirán construir conocimiento nuevo. Ambas estrategias serán usadas a lo largo de las diferentes etapas de la investigación; sin embargo, se usarán otras adicionales, de ser necesario.

Inicialmente, se buscará, seleccionará y analizará aquellos métodos (o procesos) basados en estrategias de diseño y en patrones de privacidad más relevantes. La relevancia será calificada, por ejemplo, en función de la aceptación por la comunidad de investigación, por el número de citaciones, etc. El análisis buscará determinar los tipos de instrumentos que se requieren en la experimentación en el dominio particular de estudio. Para esto se tendrá en cuenta los instrumentos que se necesitan en la experimentación en general en ingeniería de software según lo establecido en (Wohlin et al., 2012) (p.ej. el objeto, el enfoque de calidad) y los elementos que deben venir del estado del arte en el diseño respetuoso con la privacidad (p.ej. proceso de diseño, tipo de solución en los patrones).

A continuación, se buscará en la literatura elementos de los distintos tipos previamente definidos. En este sentido, se realizarán varios procesos de búsqueda organizados y planificados. El objetivo será recolectar y conformar conjuntos de elementos en forma de taxonomías, clasificaciones, etc. para cada uno de los tipos de instrumentos previamente identificados. Por ejemplo, métricas como las estrategias utilizadas o el número de patrones usados. El proceso de conformación de estos conjuntos de elementos incluirán el análisis y creación de las categorías de las taxonomías, clasificaciones, repositorios, etc., además de la inclusión fundamentada de los diferentes elementos a dichas categorías (mapeo). Asimismo, se realizará un análisis de los elementos de aquellos tipos faltantes que no se hayan encontrado en la búsqueda previa.

Se construirá una herramienta de software que soporte el proceso de experimentación al usar estrategias de diseño y patrones de privacidad. Los requisitos para la construcción del software se obtendrán del análisis de los métodos que se realizará inicialmente. Esta herramienta constará de una interfaz para el experimentador y para los participantes, y procurará ser reusable para el tipo de métodos investigados (yendo así un paso delante de las herramientas existentes en otros dominios que son específicas a los experimentos) (Riaz, Breaux & Williams, 2015). La construcción se realizará usando un proceso de desarrollo de software iterativo e incremental. La construcción de la herramienta de software se llevará a cabo durante la dirección de al menos un trabajo de titulación de pregrado.

Para validar los conjuntos de instrumentos y la herramienta elaborada, se llevará a cabo una prueba de concepto. Para ello, se usarán los conjuntos de elementos creados para diseñar un experimento controlado con todos los instrumentos necesarios. Esto permitirá validar los conjuntos de instrumentos propuestos. La información del diseño del experimento será subida a

la herramienta a construirse. Se probará el correcto funcionamiento de la herramienta tanto en la interfaz del experimentador como de los participantes.

Bibliografía (Normas APA)

Agencia Española de Protección de Datos. (2019). *A Guide to Privacy by Design*.
Asamblea Nacional del Ecuador (2019). Proyecto de Ley Orgánica de Protección de Datos Personales. Tr. 379637 https://observatoriolegislativo.ec/legislacion/proyectos-de-ley/proyecto-de-ley-organica-de-proteccion-de-datos-personales-tr-379637_76417
Cadwalladr, C., & Graham-Harrison, E. (2018). *Revealed: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach*. The Guardian. https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
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
Chung, E. S., Hong, J. I., Lin, J., Prabaker, M. K., Landay, J. A., & Liu, A. L. (2004). *Development and evaluation of emerging design patterns for ubiquitous computing*. Proceedings of the 2004 Conference on Designing Interactive Systems Processes, Practices, Methods, and Techniques - DIS '04, 233–242.
Clarke, R. (1997). *Introduction to dataveillance and information privacy, and definitions of terms*. http://rogerclarke.com/DV/Intro.html
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
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
Drozd, O. (2016a). *Catalog of Privacy Patterns*. http://privacypatterns.wu.ac.at:8080/catalog/
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 Data Protection Regulation)
Finn, R. L., Wright, D., & Friedewald, M. (2013). *Seven Types of Privacy*. In European Data Protection: Coming of Age (pp. 3–32). Springer Netherlands. https://doi.org/10.1007/978-94-007-5170-5_1
Fischer-Hübner, Simone, Köffel, C., Pettersson, J.-S., Wolkerstorfer, P., Graf, C., Holtz, L. E., König, U., Hedbom, H., & Kellermann, B. (2010). *HCI Pattern Collection – Version 2*. Privacy and Identity Management in Europe for Life.
Gamma, E., Helm, R., Johnson, R., & Vlissides, J. (1995). *Design Patterns : Elements of Reusable Object-Oriented Software*. Addison-Wesley.
Glaser, B. G., & Strauss, A. L. (2017). *Discovery of grounded theory: Strategies for qualitative research*. In Routledge. Taylor and Francis. https://doi.org/10.4324/9780203793206
Hafiz, M. (2013). *A pattern language for developing privacy enhancing technologies*. Software - Practice and Experience, 43(7), 769–787. https://doi.org/10.1002/spe.1131
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
Kalloniatis, C., Kavakli, E., & Gritzalis, S. (2008). *Addressing privacy requirements in system design: The PriS method*. Requirements Engineering, 13(3), 241–255. https://doi.org/10.1007/s00766-008-0067-3
Kuneva, M. (2009). *Roundtable on Online Data Collection*, Targeting and Profiling. European Consumer Commissioner. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156
Kung, A. (2014). *PEARs: Privacy enhancing architectures*. In B. Preneel & D. Ikonomou (Eds.), Privacy Technologies and Policy. APF 2014. Lecture Notes in Computer Science (Vol. 8450, pp. 18–29). Springer, Cham. https://doi.org/10.1007/978-3-319-06749-0_2
La Revista. (25 de agosto de 2020). El proyecto de Ley de Protección de Datos Personales en Ecuador. El Universo. Recuperado de

https://www.eluniverso.com/larevista/2020/08/24/nota/7953820/datos-personales-ley-ecuador
Lenhard, J., Fritsch, L., & Herold, S. (2017). *A literature study on privacy patterns research*. Proceedings of the 43rd Euromicro Conference on Software Engineering and Advanced Applications, 194–201. https://doi.org/10.1109/SEAA.2017.28
Ministerio de Telecomunicaciones y de la Sociedad de la Información del Ecuador. (2019). Ministro Michelena entregó proyecto de Ley Protección de Datos Personales al presidente de la Asamblea Nacional. Recuperado de https://www.telecomunicaciones.gob.ec/ministro-michelena-entrego-proyecto-de-ley-proteccion-de-datos-personales-al-presidente-de-la-asamblea-nacional/
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).
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
Pearson, S., & Benameur, A. (2011). *A decision support system for design for privacy*. In S Fischer-Hübner, P. Duquenoy, M. Hansen, R. Leenes, & G. Zhang (Eds.), Privacy and Identity Management for Life. Privacy and Identity 2010. IFIP Advances in Information and Communication Technology (Vol. 352). Springer, Berlin, Heidelberg.
Pearson, S., & Shen, Y. (2010). *Context-aware privacy design pattern selection*. In S. Katsikas, J. Lopez, & M. Soriano (Eds.), Trust, Privacy and Security in Digital Business. TrustBus 2010. Lecture Notes in Computer Science (Vol. 6264, pp. 69–80). Springer, Berlin, Heidelberg.
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
Riaz, M., Breaux, T., & Williams, L. (2015). *How have we evaluated software pattern application? A systematic mapping study of research design practices*. In Information and Software Technology (Vol. 65, pp. 14–38). Elsevier. https://doi.org/10.1016/j.infsof.2015.04.002
Romanosky, S., Acquisti, A., Hong, J., Cranor, L. F., & Friedman, B. (2006). *Privacy patterns for online interactions*. Proceedings of the 2006 Conference on Pattern Languages of Programs - PLoP '06, 1–9. https://doi.org/10.1145/1415472.1415486
Sadicoff, M., Larrondo-Petrie, M. M., & Fernández, E. B. (2005). *Privacy-aware network client pattern*. Proceedings of the Conference on Pattern Languages of Programs - PLoP.
Schumacher, M. (2003). *Security Engineering with Patterns: Origins, Theoretical Model, and New Applications*. Springer. https://doi.org/10.1007/b11930
Schümmer, T. (2004). *The public privacy - patterns for filtering personal information in collaborative systems*. Proceedings of CHI Workshop on Human-Computer-Human-Interaction Patterns, 1–35.
TNS Political & Social. (2016). *Flash Eurobarometer 443: Report e-Privacy*.
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

14. INFRAESTRUCTURA Y EQUIPOS

- *Indicar la infraestructura y equipos **disponibles** para la ejecución del proyecto, con la ubicación actual de los mismos*

N/A.

Dada la naturaleza y alcance del proyecto, se usarán los equipos portátiles de los investigadores.

Infraestructura	**Equipos**	
Laboratorio	**Nombre del Equipo**	**Ubicación del Equipo**

15. MONTO REQUERIDO

Este proyecto es sin financiamiento.

15.1 Monto y justificación del equipo requerido
N/A
15.2 Monto y justificación del personal requerido
N/A
15.4 Monto y justificación de los investigadores invitados
N/A
15.5 Monto y justificación de los viajes y salidas del campo requeridos
N/A

16. FONDOS ADICIONALES

- *Otros fondos de otros organismos (si los hubiere)*

N/A

B. DATOS INFORMATIVOS

1. INFORMACIÓN DEL DIRECTOR, CODIRECTOR, COLABORADORES Y COLABORADORES TÉCNICOS

Apellidos y nombres	No. de Cédula	HSS*	Departamento	Rol	Título de mayor nivel y mención.
Caiza Ñacato Julio César	1717824450	8	Departamento en Electrónica, Telecomunicaciones y Redes de Información	Director	Máster Universitario en Ingeniería de Redes y Servicios Telemáticos.
López Fonseca Gabriel Roberto	1715629059	4	Departamento en Electrónica, Telecomunicaciones y Redes de Información	Colaborador	Master of Science Information Systems Security

* HSS =Horas Semana Semestre: Es el número de horas que se dedica por semana a la investigación. Este número de horas se mantiene para todo el semestre

C. DECLARACIÓN FINAL
DECLARACIÓN DEL DIRECTOR DEL PROYECTO

El equipo de investigadores, representado por el Director del Proyecto declara lo siguiente:

- Que el presente proyecto es una creación original de mi autoría y del equipo de investigadores, y por tanto asumimos la completa responsabilidad legal en caso de que un tercero alegue la titularidad de los derechos intelectuales del proyecto, exonerando a la EPN de cualquier acción legal que se derive por esta causa.

- Que el presente proyecto no ha sido presentado en ninguna convocatoria de otra institución pública o privada. El incumplimiento será causal para que el proyecto no sea tomado en consideración.

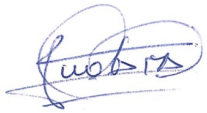
- Que si el proyecto genera algún producto o procedimiento susceptible de obtener derechos de propiedad intelectual, de los cuales se deriven beneficios, aceptamos que éstos serán

compartidos entre los investigadores y la institución o las instituciones participantes en el proyecto, conforme a lo establecido en el COESC.

- Que el equipo de investigadores y/o instituciones participantes se comprometen a mantener la confidencialidad de la información si ésta podría ser susceptible de protección por patentes, y solicitar la valoración de propiedad intelectual respectiva previa a cualquier publicación o difusión.

- Que para el caso de derechos de autor otorgamos una licencia de uso exclusivo con fines académicos para la o las instituciones participantes en el proyecto.

- Que aceptamos conocer y cumplir con la normativa vigente para la gestión de proyectos.



Firma del Director del Proyecto
Nombre: Julio César Caiza Ñacato
C.I.: 1717824450

ESCUELA POLITÉCNICA NACIONAL

VICERRECTORADO DE INVESTIGACIÓN, INNOVACIÓN Y VINCULACIÓN

Proyecto de Investigación Interno

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO

Título del Proyecto: **Soporte a la experimentación en el diseño de sistemas respetuosos con la privacidad**

Nº	Actividad	AÑO 1																																																
		Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6				Mes 7				Mes 8				Mes 9				Mes 10				Mes 11				Mes 12			
		1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
1	**Analizar los métodos de diseño de sistemas respetuosos con la privacidad basados en estrategias y patrones, y el proceso de experimentación aplicado a ellos.**																																																
1.1	Búsqueda y selección de métodos o procesos a estudiar.																																															
1.2	Análisis de métodos o procesos seleccionados.																																															
1.3	Definición de tipos de instrumentos necesarios.																																															
1.4	*Informe sobre el análisis de los métodos de diseño de sistemas respetuosos con la privacidad que están basados en estrategias y patrones, y sobre el proceso de experimentación con ellos*																																															
2	**Generar un conjunto de instrumentos reusables para llevar a cabo experimentos con el tipo de métodos previamente analizados.**																																															
2.1	Planificación de búsqueda en la literatura por cada tipo de instrumento.																																															
2.2	Búsqueda en la literatura por cada tipo de instrumento.																																															
2.3	Análisis de resultados por cada tipo de instrumento.																																															
2.4	Composición de categorías de clasificaciones, taxonomías o elementos necesarios.																																															
2.5	Mapeo de elementos encontrados a las clasificaciones y taxonomías.																																															
2.6	Análisis de elementos de tipos de instrumentos faltantes.																																															
2.7	*Un conjunto de instrumentos reusables para la experimentación con el tipo de métodos estudiados.*																																															
3	**Desarrollar una herramienta que brinde soporte a la experimentación con el tipo de métodos analizados en este proyecto.**																																															
3.1	Identificación de requerimientos considerando los métodos o procesos basados en estrategias y patrones y el proceso de experimentación.																																															
3.2	Análisis y diseño. Estas actividades será iterativas hasta culminar el producto (herramienta de software)																																															
3.3	Implementación																																															
3.4	Pruebas y validación																																															
3.5	*Una herramienta de software que brinde soporte a la experimentación con métodos de diseño basados en estrategias y patrones y donde se haga uso de los instrumentos previamente creados.*																																															
3.6	*Un trabajo de titulación de pregrado donde se desarrolle la herramienta de software.*																																															
4	**Validar el soporte a la experimentación provisto a través de una prueba de concepto.**																																															
4.1	Diseño de un experimento de prueba.																																															
4.2	Puesta en marcha del experimento de prueba en la herramienta.																																															
4.3	Pruebas de la herramienta durante la puesta en marcha del experimento.																																															
4.4	*Un reporte de una prueba de concepto*																																															
5	**Divulgar los resultados y la temática investigada.**																																															
2.1	Escritura de artículo reportando resultados.																																															
2.2	Elaboración de presentaciones para charlas abiertas																																															
2.3	*El envío de un artículo o presentación en congreso (indexados en Scopus, Scielo o WoS) reportando los resultados científicos alcanzados.*																																															
2.4	*La presentación de la temática, su necesidad e importancia y de los resultados alcanzados a través de charlas abiertas.*																																															