INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año VII. Vol VII. N°12. Enero – Junio. 2025
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

https://doi.org/10.35381/i.p.v7i12.4471

Protección de datos por diseño y por defecto. Implicaciones legales en el desarrollo de software

Data protection by design and by default. Legal implications in software development

Joselyn Gabriela Castro-Paredes
jcastro12@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0009-0001-4558-8739

George Richard Mendoza-Masache
gmendoza4@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0009-0007-6890-5614

Nancy Magaly Loja-Mora
nmloja@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0000-0002-5583-4278

Harold Patricio Loján-Alvarado
hlojan@utmachala.edu.ec
Universidad Técnica de Machala, Machala, El Oro
Ecuador
https://orcid.org/0009-0008-6869-261X

Recibido: 15 de septiembre de 2024
Revisado: 03 de octubre de 2024
Aprobado: 15 de diciembre de 2024
Publicado: 01 de enero de 2025

INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año VII. Vol VII. N°12. Enero – Junio. 2025
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.

RESUMEN

El objetivo de este estudio es aplicar los principios de protección de datos por diseño y por defecto en el desarrollo de una aplicación móvil para la gestión de parqueos, incorporando medidas de seguridad alineadas con la “Ley Orgánica de Protección de Datos Personales de Ecuador”. La metodología aplicada fue Scrum, adaptada para integrar no solo aspectos técnicos, sino también requisitos legales. Como resultado, desarrollo de una aplicación móvil para el control de parqueos donde se incorporaron funcionalidades alineadas con la normativa, lo cual permitió comunicar de forma transparente la recolección y uso de la información generando una percepción positiva de seguridad y aceptación por parte de los usuarios. Esto permite incorporar la protección de datos por diseño y por defecto desde el inicio del desarrollo, cumplir con la normativa vigente, fortalecer la confianza de los usuarios y garantizar una mayor calidad legal y técnica del producto final.

Descriptores: Protección de datos; datos personales; desarrollo de software; Scrum. (Tesauro UNESCO).

ABSTRACT

The objective of this study is to apply the principles of data protection by design and by default in the development of a mobile application for parking management, incorporating security measures aligned with the Organic Law on Personal Data Protection of Ecuador. The methodology applied was Scrum, adapted to integrate not only technical aspects but also legal requirements. The result was the development of a mobile application for parking management that incorporated regulatory-aligned features. This allowed for transparent communication about the collection and use of information, generating a positive perception of security and user acceptance. This allowed us to incorporate data protection by design and by default from the beginning of development, comply with current regulations, strengthen user trust, and guarantee higher legal and technical quality of the final product.

Descriptors: Data Protection; personal data; software development; Scrum. (UNESCO Thesaurus).

INTRODUCCIÓN

La seguridad en el desarrollo de software ha sido tradicionalmente abordada como un complemento tardío, implementándose durante la programación mediante medidas técnicas o en fases finales, como la etapa de pruebas. Los enfoques tradicionales en seguridad de software suelen tratarla como un complemento añadido en etapas posteriores, lo cual ha demostrado ser insuficiente para garantizar sistemas verdaderamente seguros desde su concepción. La razón es simple, en entornos ágiles a gran escala, la presión por entregar productos rápidamente puede relegar la seguridad a un segundo plano (Moyón et al., 2021).

En Ecuador, esta situación se agrava por la escasa cultura en seguridad de la información. Barahona-Martínez et al., (2024) identifican entre las problemáticas más comunes: filtraciones de bases de datos, vigilancia digital masiva, uso encubierto de datos personales y falta de consentimiento informado. Frente a este panorama, Von Grafenstein et al. (2022) sostienen que “la implementación efectiva de la mayoría de las disposiciones del Reglamento General de Protección de Datos (RGPD) presupone una especificación eficaz de los fines del tratamiento” (p. 3). Además, enfatizan que el cumplimiento normativo solo puede alcanzarse si los sistemas se desarrollan desde una perspectiva interdisciplinaria, es decir, integrando aspectos legales, técnicos y de experiencia de la entidad bancaria.

En Polonia una entidad bancaria fue multada con 928.498,06 euros por no informar adecuadamente a los clientes sobre una violación de datos personales, infringiendo el artículo 34 del RGPD. El banco argumentó que los datos fueron enviados por error a una institución considerada de confianza, pero la autoridad concluyó que la falta de notificación a los afectados representaba una desatención grave a sus derechos, impidiéndoles tomar medidas para mitigar posibles consecuencias negativas (*Polish Data Protection Authority* (UODO), 2025).

Frente a estos desafíos, los principios de protección de datos por diseño y por defecto emergen como estrategias normativas y técnicas fundamentales. Reconocidos por el artículo 25 del Reglamento General de Protección de Datos (RGPD) y por el artículo 39 de la Ley Orgánica de Protección de Datos Personales (LOPDP) en Ecuador, estos principios exigen la incorporación de medidas de seguridad desde las fases iniciales de cualquier proyecto que implique tratamiento de datos personales. A nivel nacional, el Reglamento de la LOPDP en sus artículos 59 y 60, establece que dichas medidas deben considerar la naturaleza del tratamiento, los riesgos y el estado del arte, limitando el procesamiento de datos únicamente a lo estrictamente necesario (Asamblea Nacional, 2021; Presidencia de la República, 2023).

Zambrano et al. (2024) destacan que contar con un marco normativo claro permite asignar responsabilidades ante vulneraciones de datos personales, lo que refuerza la importancia de aplicar medidas legales y técnicas desde el inicio del desarrollo. Varios estudios en Ecuador evidencian la urgencia de aplicar estos principios. Copara Suárez (2024) reveló que muchas aplicaciones móviles carecen de políticas de protección de datos transparentes y ajustadas a la normativa. En un enfoque complementario, Adriano Moromenacho (2024) propuso la integración de controles de seguridad basados en la metodología DevSecOps en aplicaciones gubernamentales.

Por su parte, Lange & Kunz (2024) diseñaron una arquitectura basada en el ciclo de vida de desarrollo seguro de Microsoft (SSDLC) para entidades públicas, destacando la necesidad de limitar el acceso y mitigar el uso indebido de datos Esta visión se complementa con la propuesta de Landa Reza (2024), quien subraya que “desde el diseño inicial o creación y el desarrollo de un instrumento tecnológico, se ha de tener en consideración el derecho a la protección de datos como un elemento indispensable”, destacando que esta obligación se extiende a lo largo de todo el ciclo de vida del sistema, desde su concepción hasta su retirada.

En el plano jurídico, Cornejo Ramos y Sánchez (2023) advierten que, a pesar de los avances normativos, persisten vacíos legales en la aplicación práctica de la LOPDP frente a delitos informáticos. Esto plantea la necesidad de modelos de desarrollo que integren la normativa desde etapas tempranas.

En este sentido, el presente artículo tiene como objetivo aplicar los principios de protección de datos por diseño y por defecto en el desarrollo de una aplicación móvil para la gestión de parqueos, incorporando medidas de seguridad alineadas con la LOPDP. Para ello, se adopta la metodología ágil Scrum, garantizando la integración iterativa de requisitos legales, funcionales y técnicos a lo largo del ciclo de vida del software.

MÉTODO

Para el desarrollo de este trabajo se adoptó la metodología ágil Scrum, estructurando sus fases de manera que incorporen actividades orientadas al cumplimiento de la LOPDP.

Scrum es una metodología ágil ampliamente utilizada en el desarrollo de software, que permite gestionar proyectos de forma iterativa e incremental, adaptándose a cambios en los requisitos durante el ciclo de vida del producto. Su estructura está basada en sprints, los cuales son periodos de tiempo definidos en los que se desarrollan incrementos funcionales del producto (Schwaber y Sutherland, 2020).

Cada sprint incluye eventos clave como la planificación, reuniones diarias, revisión y retrospectiva, que garantizan la entrega continua de valor y la mejora del proceso (Chang y Shokrolah Shirazi, 2022). Los principales roles en Scrum son el Scrum Master, quien guía al equipo y vela por el cumplimiento de la metodología; el Product Owner, encargado de comunicar la visión del producto y priorizar el backlog; y el equipo de desarrollo, responsable de implementar las funcionalidades.

El proceso se organizó en cuatro etapas principales, conforme a la Guía de Scrum:

- **Fase de planificación*:*** Durante la fase de planificación se analizaron los artículos relevantes de la LOPDP y su Reglamento, con el objetivo de identificar las

obligaciones legales que debían ser integradas en el sistema. A partir de ello, se definieron historias de usuario orientadas al cumplimiento normativo, tales como la gestión del consentimiento, el ejercicio de derechos de los titulares y la implementación de medidas de seguridad. Se organizó el backlog del producto priorizando estas funcionalidades, y se asignaron los roles de Scrum, considerando al Product Owner como responsable de velar por el cumplimiento legal del proyecto. Además, se diseñó una arquitectura inicial con principios como: minimización de datos, cifrado, anonimización y control de acceso.

- ***Fase de desarrollo:*** En la fase de desarrollo se incluyeron mecanismos para gestionar el consentimiento del usuario (art. 8 y 10), permitiendo otorgarlo, modificarlo o revocarlo en cualquier momento mediante una interfaz clara y accesible. También se desarrollaron las opciones para ejercer los derechos de rectificación, actualización, eliminación, oposición y suspensión del tratamiento (art. 14, 15, 16 y 19), incluyendo la posibilidad de modificar o eliminar datos desde la aplicación, asegurando su eliminación efectiva bajo el principio de minimización.
  En cumplimiento del artículo 27, “Protección de datos personales de personas fallecidas”, se habilitó la opción para que los titulares de derechos sucesorios, las personas autorizadas por el titular en vida o los representantes legales, según corresponda, puedan solicitar el acceso, actualización o eliminación de los datos personales del usuario fallecido. Asimismo, se incluyó la funcionalidad para eliminar de forma definitiva dicha información, una vez que se haya reportado el fallecimiento y se presente la respectiva acta de defunción.
  En seguridad, se aplicaron controles de acceso por rol, registros de actividad y bloqueo automático tras intentos fallidos de ingreso, garantizando que solo usuarios autorizados accedan a los datos personales. Además, se implementó un mecanismo de seudonimización mediante cifrado AES-256 en el backend, que impide la exposición directa de información identificadora en los registros.

- ***Fase de revisión:*** En la fase de revisión se evaluaron las funcionalidades desarrolladas, verificando su correcto funcionamiento y su adecuación a los requisitos establecidos en la fase de planificación. Se validó el comportamiento de las interfaces de consentimiento, los mecanismos de ejercicio de derechos por parte del usuario, y los controles de acceso. Esta evaluación permitió detectar errores, inconsistencias o mejoras necesarias en la lógica de tratamiento de datos, que fueron documentadas y priorizadas para ser abordadas en el siguiente ciclo de desarrollo. La revisión se realizó de forma colaborativa entre los miembros del equipo, asegurando retroalimentación inmediata y enfoque en la mejora continua.
- ***Fase de retrospectiva:*** Para el cierre del sprint, se realizó una sesión de retrospectiva con el equipo de desarrollo para evaluar el proceso e implementación de las funcionalidades descritas. La fase permitió identificar desafíos y oportunidades de mejora en el ciclo del desarrollo. Se aplicó una validación externa mediante entrevistas a cinco personas que no tienen formación en tecnología, pero poseen un vehículo, como posibles usuarios. Las respuestas permitieron identificar percepciones sobre la claridad en el tratamiento de datos, la cantidad de información solicitada, la facilidad para modificar datos personales y la accesibilidad para eliminar la cuenta. Los resultados se utilizaron para validar la experiencia de usuario y ajustar aspectos funcionales en ciclos posteriores.

RESULTADOS

Según el Instituto Nacional de Estándares y Tecnología (NIST) de Estados Unidos, adoptar prácticas de desarrollo de software seguro desde las primeras etapas permite reducir el número de vulnerabilidades, mitigar el impacto de las no detectadas y abordar sus causas raíz para prevenir futuras recurrencias (Souppaya et al., 2022).

Para este fin, la protección de datos por diseño y por defecto implica aplicar principios como la minimización y la seudonimización desde las fases iniciales del desarrollo. Según

Drev y Delak (2022), este enfoque no solo limita la recopilación y retención innecesaria de datos, sino que también promueve el cumplimiento integral de los principios básicos de protección, incluyendo la evaluación de impacto.

Fase de planificación

Como primer paso y de acuerdo con el principio de minimización de datos, se detalla a continuación la información solicitada al usuario, la cual ha sido limitada a lo necesario para el funcionamiento de la aplicación:

- Correo electrónico: para identificación y recuperación de cuenta.
- Nombres y apellidos: asociar las transacciones de parqueo e identificar al titular.
- Cédula de identidad: requisito para validar la autenticidad del usuario.

La justificación para la recolección de estos datos está explícitamente descrita en los términos y condiciones de uso de la aplicación, los cuales son accesibles antes del registro y en cualquier momento durante su utilización.

A fin de definir el product backlog, se identificaron los requisitos esenciales del sistema, los cuales se clasificaron en dos categorías. En la Tabla 1 se presentan los requisitos no funcionales, relacionados con aspectos de seguridad, privacidad, rendimiento y cumplimiento normativo.

Tabla 1.
Requisitos no funcionales.

Código	Requisito	Descripción
RNF01	Autenticación segura	Contraseñas cifradas y verificación vía correo electrónico para acceso seguro.
RNF02	Control de acceso basado en roles	Los permisos se definen según el rol del usuario, limitando el acceso a datos personales.
RNF03	Minimización técnica de datos	Estructura de base de datos y lógica de aplicación diseñada para recolectar y tratar solo los datos necesarios.
RNF04	Protección por defecto	La configuración del sistema evita por defecto cualquier exposición innecesaria de datos personales.
RNF05	Registro de accesos y operaciones	Se guarda un historial de acciones sobre los datos personales para auditoría y control.
RNF06	Aplicación de seudonimización	El sistema debe separar los datos identificativos (cédula, correo electrónico, contraseña) de las operaciones internas mediante identificadores únicos.

Elaboración: Los autores.

Por su parte, la tabla 2 recoge los requisitos funcionales, correspondientes a las acciones y características específicas que debe ofrecer la aplicación para cumplir con los principios de protección de datos por diseño y por defecto.

Tabla 2.
Requisitos funcionales.

Código	Requisito	Descripción	Referencia LOPDP
RF01	Registro de usuario	Permite al usuario crear una cuenta ingresando solo los datos mínimos necesarios.	Art. 8, Art. 9
RF02	Gestión de consentimiento	Permite al usuario aceptar, modificar o revocar el consentimiento sobre el uso de sus datos personales.	Art. 8, Art.10, Art. 16
RF03	Visualización de datos personales	Muestra al usuario sus datos personales de forma clara y accesible.	Art. 13
RF04	Rectificación de datos	Permite la modificación de información personal incorrecta o desactualizada.	Art. 14
RF05	Eliminación de cuenta	El usuario puede solicitar eliminar su cuenta, y sus datos deben ser eliminados de forma definitiva.	Art. 15
RF06	Descarga de información	El sistema debe permitir al usuario descargar un archivo con todos sus datos.	Art. 17
RF07	Feedback del usuario	El usuario puede reportar errores y dejar comentarios.	Art. 10(c. Transparencia)
RF08	Gestión de datos de personas fallecidas	Permitir que el usuario pueda ceder sus datos o eliminar su cuenta en caso de fallecer.	Art. 27

Elaboración: Los autores.

Fase de desarrollo

La Figura 1 presenta la arquitectura lógica de la aplicación desarrollada, estructurada en tres componentes principales: frontend, backend y base de datos. Este diseño permite gestionar el tratamiento de datos personales conforme a los principios de protección por diseño. Se destacan mecanismos como la seudonimización aplicada en el backend mediante cifrado AES-256, el control de acceso diferenciado por roles, la encriptación de los datos en tránsito (HTTPS) y en reposo (PostgreSQL), así como la trazabilidad de acciones basada en identificadores no sensibles.

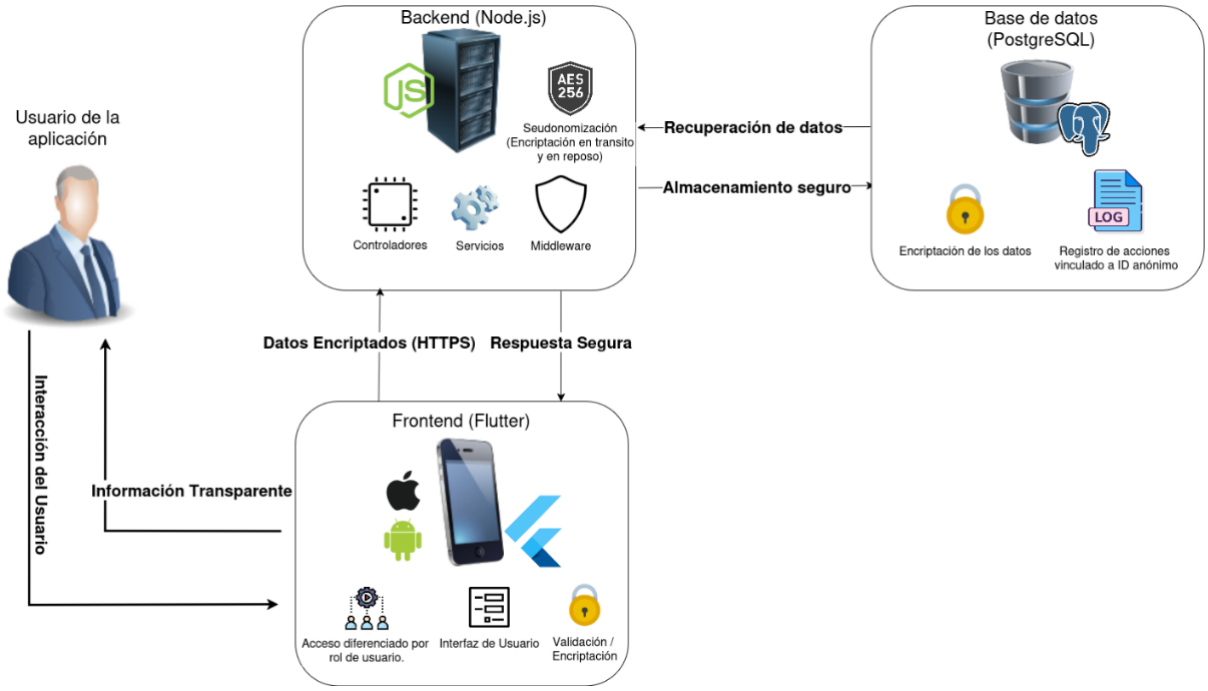

Figura 1. Arquitectura lógica de la aplicación con enfoque de protección de datos por diseño y por defecto.
Elaboración: Los autores.

Fase de revisión

La Figura 2 muestra las pantallas clave de la aplicación relacionadas con el registro, actualización y eliminación de datos personales. En la interfaz de registro se informa claramente sobre los datos solicitados y se incluye un enlace directo a los términos y condiciones, en línea con lo dispuesto en el artículo 10, literal e) y el artículo 8 de la LOPDP. Las pantallas de edición y actualización de datos personales, como nombres o correo electrónico, se alinean con el ejercicio del derecho de rectificación (art. 14), mientras que la opción de eliminación de cuenta responde al derecho de supresión establecido en el artículo 15 de la misma ley.

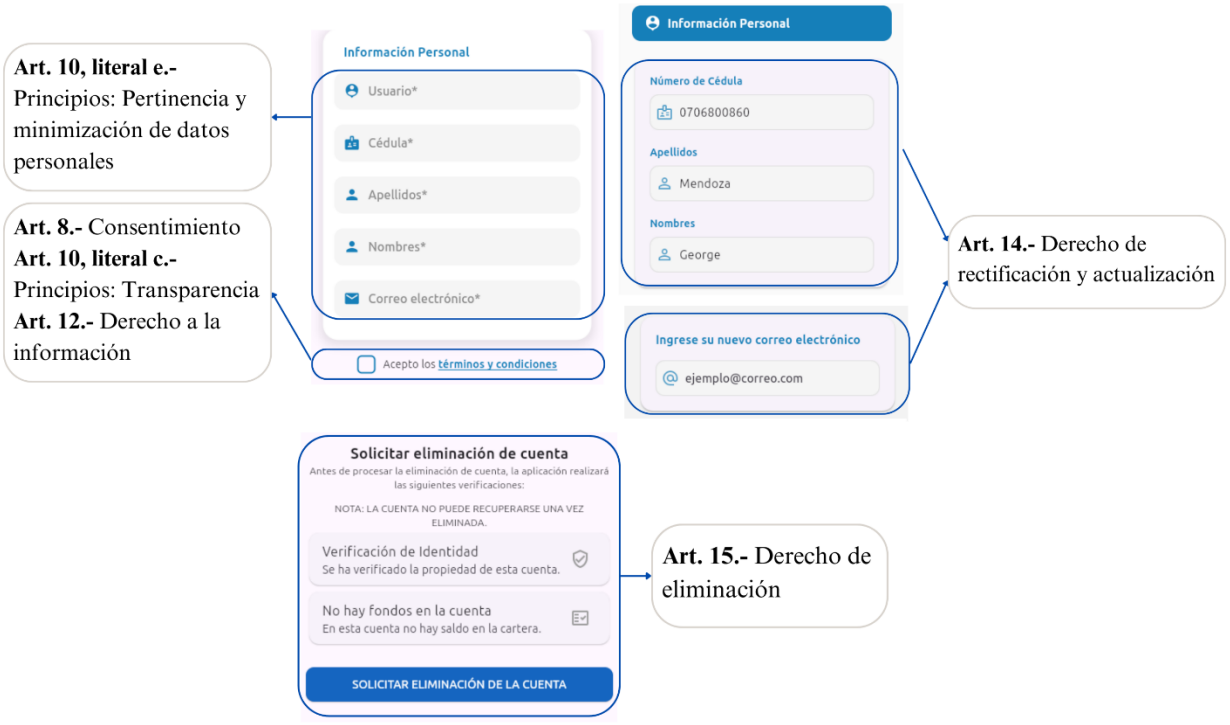

Figura 2. Interfaz de usuario para registro, rectificación y eliminación de datos personales.
Elaboración: Los autores.

Adicionalmente se desarrollan las secciones de Política de Privacidad y Términos y Condiciones de la aplicación. Ambos documentos están disponibles al usuario desde el inicio de su interacción con el sistema y fueron elaborados conforme a los principios de transparencia y finalidad establecidos en el artículo 10, literales c) y d) de la LOPDP. En ellos se detalla de forma clara el tipo de datos personales que se recopilan, su propósito específico, y el marco legal aplicable, permitiendo que el usuario tome decisiones informadas respecto al uso de la aplicación y el tratamiento de su información.

Por otra parte, la figura 4 presenta funcionalidades adicionales que refuerzan la protección de los derechos del titular de los datos. Se incluye la opción para oponerse al tratamiento de información personal (art. 15), así como mecanismos para enviar retroalimentación y reportar errores, lo cual se enmarca en el principio de transparencia (art. 10, literal e). Además, se implementa la posibilidad de descargar la información personal registrada en la aplicación, permitiendo ejercer el derecho a la portabilidad conforme al artículo 17 de la LOPDP.

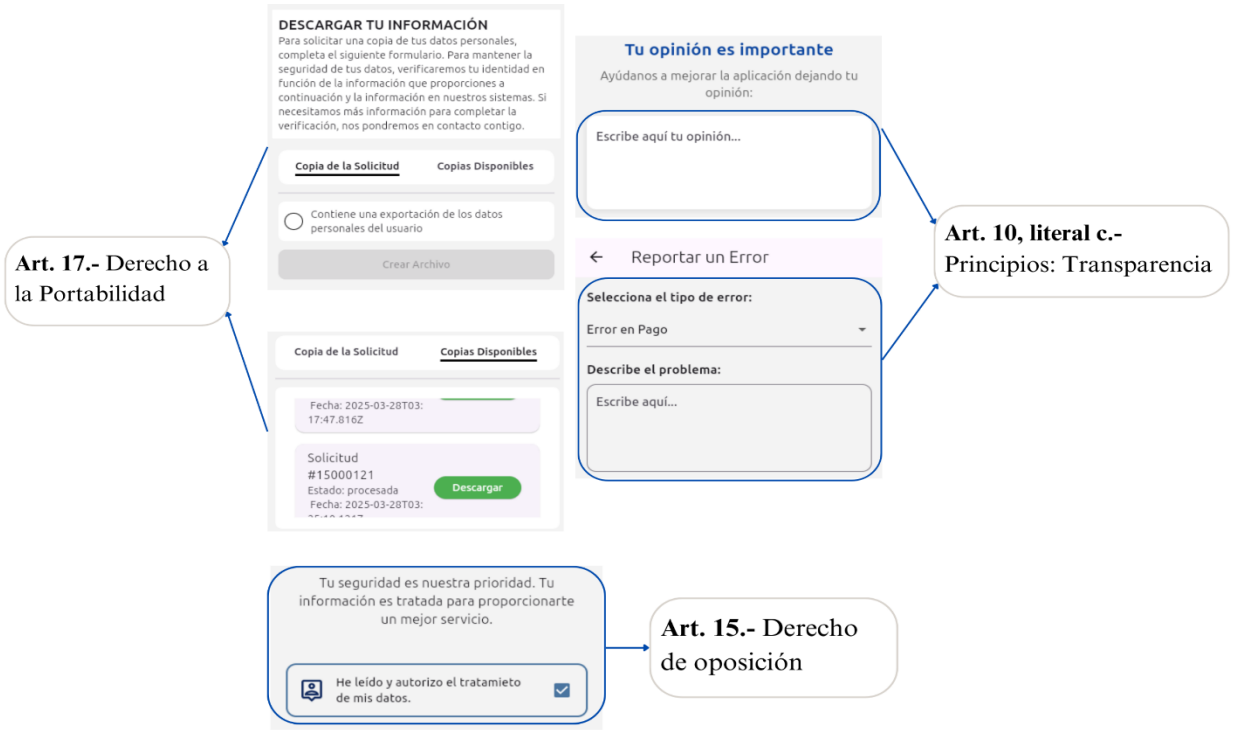

Figura 4. Funcionalidades de oposición, retroalimentación, reporte de errores y descarga de información.
Elaboración: Los autores.

Fase de retrospectiva

En esta fase se identificaron mejoras clave en dos ámbitos fundamentales: el proceso de desarrollo y la experiencia de usuario. A nivel interno, se detectó la necesidad de documentar con mayor precisión los flujos de datos personales y de considerar estrategias más robustas para la gestión de dichos datos, garantizando en todo momento la privacidad y seguridad del usuario.

En cuanto a la validación externa, los participantes expresaron una actitud positiva respecto a la claridad en el tratamiento de sus datos, destacando que los documentos sobre política de privacidad y términos y condiciones eran comprensibles, concisos y accesibles, a diferencia de textos excesivamente largos o confusos. No obstante, algunos

señalaron que sería útil contar con recordatorios más visibles sobre sus derechos, especialmente en lo referente a la rectificación y eliminación de información.

Durante las entrevistas, surgió además una duda relevante sobre el ciclo de vida de los datos. Al considerar distintos escenarios, como el fallecimiento del usuario, tres participantes manifestaron preocupación sobre qué sucedería con su información en ese caso. Esto motivó la implementación de lo establecido en el Art. 27 de la Ley Orgánica de Protección de Datos Personales (LOPDP), referente a los datos personales de personas fallecidas (Asamblea Nacional, 2021). Se elaboró una política que contempla la eliminación o el traspaso de datos conforme a los deseos previamente expresados por el titular, con verificación por documentación legal de un representante autorizado.

Gracias a estos aportes, se reforzaron medidas relacionadas con la accesibilidad para eliminar la cuenta, se mejoraron los textos informativos dentro de la aplicación y se establecieron lineamientos para el tratamiento de datos en caso de fallecimiento, fortaleciendo así el cumplimiento de la normativa vigente.

DISCUSION

El objetivo del trabajo es aplicar los principios de protección de datos por diseño y por defecto en el desarrollo de una aplicación móvil para la gestión de parqueos, incorporando medidas de seguridad alineadas con la LOPDP. Para Salazar-Salazar et al. (2024), el Ciclo de Vida del Software (SDLC, por sus siglas en inglés) se define como el conjunto de procesos que se utilizan para especificar y transformar los requerimientos del usuario en un producto de software funcional; incluye actividades como la recolección de requerimientos, diseño, implementación, pruebas, despliegue y mantenimiento del software, las cuales pueden realizarse de manera secuencial, iterativa o simultáneamente, dependiendo del modelo adoptado.

Ann Cavoukian señaló que los responsables del tratamiento de datos personales deberían, desde el inicio de la planificación, considerar medidas que permitan alcanzar

los objetivos legítimos del tratamiento de la manera menos invasiva posible para la privacidad de las personas (Cavoukian, 2009). Por su parte, Bygrave (2017) explica que la protección de datos por defecto requiere que el responsable del tratamiento implemente medidas técnicas y organizativas adecuadas para garantizar que, por defecto, solo se procesen los datos personales necesarios para cada propósito específico del tratamiento.

Para el desarrollo del proyecto se organizó en cuatro etapas principales, conforme a la Guía de Scrum: planificación, desarrollo, revisión y retrospectiva. Durante la primera fase, planificación, se identificaron los requisitos funcionales y no funcionales del sistema. Determinándose que datos recolectar y las diferentes tareas del backlog.

La seudonimización es una técnica que protege la identidad del titular mediante la separación de los datos de identificación directa y su sustitución por códigos o seudónimos (Bygrave, 2017; Beumier & Debatty, 2025). Esta se aplica en la segunda fase, mediante cifrado AES-256 El cifrado constituye un proceso que convierte los datos en un formato ilegible para quienes no posean una clave de descifrado autorizada, permite que, incluso en caso de una violación de seguridad, los datos permanezcan ininteligibles para terceros no autorizados (González Hernández, 2023).

Otras funciones incluidas en esta etapa de desarrollo es el control de acceso diferenciado por roles, la encriptación de los datos en tránsito (HTTPS) y en reposo (PostgreSQL), así como la trazabilidad de acciones basada en identificadores no sensibles.

En la tercera fase se crea la interfaz, ella comprende el registro, rectificación y eliminación de datos personales. Se muestran también las pantallas de Política de Privacidad y Términos y Condiciones. Se implementaros las funcionalidades de oposición, retroalimentación, reporte de errores y descarga de información. En la fase retrospectiva se realizan diferentes mejoras sobre todo el proceso.

Según Palacios-Alonso et al. (2021), la privacidad por diseño es un enfoque fundamental en la seguridad de los datos personales y la gobernanza digital. Su correcta

implementación en el desarrollo de sistemas tecnológicos contribuye a la estabilidad económica y social, garantizando que las plataformas digitales cumplan con estándares internacionales como los establecidos en el RGPD (Presidencia de la República, 2023).

CONCLUSIONES

El presente estudio logró satisfactoriamente el desarrollo de una aplicación móvil para el control de parqueos en Ecuador que aplique las disposiciones de la LOPDP en sus artículos 8, 9, 10, 13, 14, 16, 17 y 27, lo que constituyó el fundamento jurídico para las funcionalidades de seguridad de la solución tecnológica. Se implementó rigurosamente el principio de minimización de datos, identificando exclusivamente aquellos estrictamente necesarios para la operación de la aplicación desde la fase inicial del proyecto, lo que evidencia el cumplimiento del requisito normativo de protección por diseño y por defecto.

Tras analizar las implicaciones legales que enfrenta el desarrollo de software en Ecuador, se constató que frecuentemente se omiten consideraciones jurídicas relativas a la protección de datos personales, privilegiando exclusivamente aspectos técnicos. Esta observación se validó desde nuestra trayectoria académica, donde inicialmente se priorizaba el cumplimiento de requerimientos técnicos, sin contemplar las implicaciones legales inherentes al tratamiento de datos personales, por lo que, fue necesario adquirir conocimientos específicos sobre la normativa vigente para incorporar en la metodología Scrum las obligaciones jurídicas establecidas en la LOPDP como funcionalidades técnicas concretas para la protección de los datos personales de los usuario, lo cual subraya la necesidad imperante de incorporar formación jurídica en los programas educativos y en los procesos de desarrollo profesional de software.

Se concluye que la implementación de la protección de datos por diseño y por defecto no constituye únicamente una buena práctica en el ámbito técnico, sino que representa una obligación jurídica ineludible en el marco regulatorio del desarrollo de software en

Ecuador, constituyéndose en un elemento fundamental para garantizar los derechos de los usuarios y para el desarrollo de soluciones tecnológicas que cumplan con los criterios de responsabilidad, seguridad y conformidad legal. La metodología práctica desarrollada en este estudio podrá ser replicada en futuros proyectos de desarrollo de software que requieran el tratamiento de datos personales, contribuyendo así a la promoción de una cultura de protección de datos en la industria tecnológica ecuatoriana.

FINANCIAMIENTO

No financiado.

AGRADECIMIENTO

A todos los actores sociales involucrados en el desarrollo de la investigación.

REFERENCIAS CONSULTADAS

Adriano Moromenacho, D. F. (2024). *Propuesta de desarrollo de aplicaciones informáticas mediante un enfoque de seguridad informática en entidades gubernamentales* [Trabajo de Maestría, Universidad Tecnológica Israel]. Repositorio Digital Universidad Israel. https://n9.cl/76qck1

Asamblea Nacional. (2021). *Ley Orgánica de Protección de Datos Personales.* Pub. Registro Oficial Suplemento 459 de 26-may.-2021. https://n9.cl/9uqbl

Barahona-Martinez, G. E., Barzola-Plúas, Y. G., y Peñafiel-Muñoz, L. V. (2024). El Derecho a la Protección de Datos y el Avance de las Nuevas Tecnologías en Ecuador: Implicaciones Legales y Éticas. *Journal of Economic and Social Science Research*, *4*(3), 46-64. https://doi.org/10.55813/gaea/jessr/v4/n3/113

Beumier, C., & Debatty, T. (2025). Pseudonymisation of SS7 Identifiers by Random Tables. In *Future of Information and Communication Conference* (pp. 369-378). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-85363-0_22

Bygrave, L. A. (2017). Data Protection by Design and by Default: Deciphering the EU's Legislative Requirements. *Oslo Law Review*, 4(2), 105–133. https://doi.org/10.18261/issn.2387-3299-2017-02-03

Cavoukian, A. (2009). *Privacy by Design: The 7 Foundational Principles*. Office of the Information and Privacy Commissioner of Ontario. https://n9.cl/4aa3j

Chang, H. F., & Shokrolah Shirazi, M. (2022). Adapting Scrum for Software Capstone Courses. *Informatics in Education*, *21*, 605-634. https://doi.org/10.15388/infedu.2022.25

Copara Suárez, W. Z. (2024). *Transparencia y protección de datos en aplicaciones móviles en Ecuador: Evaluación de la difusión de políticas de protección de datos en aplicaciones móviles*. [Tesis de maestría, Escuela Politécnica Nacional]. Repositorio digital – EPN. https://n9.cl/m335ik

Cornejo Ramos, S. A., y Sánchez, D. X. (2023). La protección de datos de carácter personal frente al delito de interceptación ilegal de datos. *Código Científico Revista de Investigación*, *4*(E2), 984-1023. https://doi.org/10.55813/gaea/ccri/v4/nE2/192

Drev, M., & Delak, B. (2022). Conceptual Model of Privacy by Design. *Journal of Computer Information Systems*, *62*(5), 888-895. https://doi.org/10.1080/08874417.2021.1939197

González Hernández, I. (2023). Protección de datos y seguridad de la información. *Revista Canaria de Administración Pública*, *1*, 285-311. https://doi.org/10.36151/RCAP.2023.9

Landa Reza, I. (2024). La protección de datos desde el diseño y por defecto como obligación legal preventiva de la domótica. *Revista Electrónica de Direito*, *34*(2), 206-228. https://doi.org/10.24840/2182-9845_2024-0002_0009

Lange, F., & Kunz, I. (2024). *Evolution of secure development lifecycles and maturity models in the context of hosted solutions*. Journal of Software: Evolution and Process, 36(7), e2711. https://doi.org/10.1002/smr.2711

Moyón, F., Méndez, D., Beckers, K., Klepper, S. (2020). How to Integrate Security Compliance Requirements with Agile Software Engineering at Scale?. In: Morisio, M., Torchiano, M., Jedlitschka, A. (eds) *Product-Focused Software Process Improvement. PROFES 2020*. *Lecture Notes in Computer Science*, vol 12562. Springer. https://doi.org/10.1007/978-3-030-64148-1_5

Palacios-Alonso, D., Cousido-González, M. P., Domínguez-Mateos, F., Guillén-García, J., Ortega-delCampo, D., Conde, C., y Cabello, E. (2021). Privacidad por diseño, clave para la buena gobernanza. *Derecom*, *31*, 215-223. https://n9.cl/d792t

Polish Data Protection Authority (UODO). (2025). *Administrative fine for failure to inform data breach: mBank case (Poland).* European Data Protection Board (EDPB). https://n9.cl/k9820

Presidencia de la República. (2023). *Reglamento de la Ley Orgánica de Protección de Datos Personales*. Pub. L. No. 435, 16. https://n9.cl/b1jeg

Salazar-Salazar, G., Mora, M., Duran-Limon, H., Alvarez-Rodriguez, F., y Munoz-Zavala, A. (2024). Review of Agile SDLC for Big Data Analytics Systems in the Context of Small Organizations Using Scrum-XP. *The International Arab Journal of Information Technology*, *21*(6), 1089-1110. https://doi.org/10.34028/iajit/21/6/12

Schwaber, K., & Sutherland, J. (2020). *The Scrum Guide: The definitive guide to Scrum: The rules of the game.* https://n9.cl/31ejr

Souppaya, M., Scarfone, K., & Dodson, D. (2022). *Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities (No. NIST SP 800-218; p. NIST SP 800-218).* National Institute of Standards and Technology (U.S.). https://doi.org/10.6028/NIST.SP.800-218

Von Grafenstein, M., Jakobi, T., & Stevens, G. (2022). Effective data protection by design through interdisciplinary research methods: The example of effective purpose specification by applying user-Centred UX-design methods. *Computer Law & Security Review*, *46*, 105722. https://doi.org/10.1016/j.clsr.2022.105722

Zambrano, J., Sasintuña, J. G., y Jara Aguilar, P. (2024). Responsabilidad civil por el incumplimiento de la normativa de protección de datos personales. *USFQ Law Review*, *11*(2). https://doi.org/10.18272/ulr.v11i2.3370

INGENIUM ET POTENTIA
Revista Electrónica Multidisciplinaria de Ciencias Básicas, Ingeniería y Arquitectura
Año VII. Vol VII. N°12. Enero – Junio. 2025
Hecho el depósito de Ley: FA2019000052
FUNDACIÓN KOINONIA (F.K).
Santa Ana de Coro, Venezuela.