Marco para una Autoprotección Eficaz de la Privacidad en Entornos Móviles

M. Mercedes Martínez-González, Amador Aparicio,
Alejandro Pérez-Fuente, Pablo-Abel Criado Lozano,
Margarita Gonzalo Tasis, Quiliano Isaac Moro

Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid
gi.ingpriv@uva.es

***Resumen*—(Artículo original)**
La herramienta con la que los usuarios cuentan para autoproteger su privacidad cuando utilizan aplicaciones móviles son los ajustes de sus dispositivos. Sin embargo, la mayoría de las herramientas de análisis utilizan conceptos que no se corresponden con aquello que los usuarios pueden manejar, lo cual obstaculiza su capacidad para trasladar esos resultados en una autoprotección eficaz. En el proyecto App-PI ofrecemos herramientas pensadas para solventar esta carencia. El repositorio App-PIMD ofrece metadatos para construir indicadores que permiten evaluar la privacidad y seguridad de las aplicaciones móviles basados en conceptos asequibles para cualquier tipo de usuario, aquello sobre lo que en realidad los usuarios pueden actuar. Introducimos así el criterio de la usabilidad, lo que nos permite obtener una tecnología más humana. En este trabajo presentamos el repositorio App-PIMD y el indicador App-PIM, una métrica diseñada pensando en los usuarios, que la utilizan a través de una herramienta online, *APK Falcon*. Todos ellos están en servicio, para su uso en abierto.

***Index Terms*—Privacidad, Usuarios, Aplicaciones móviles, Autoprotección, Metadatos, Métrica, Permisos.**

I. Introducción

Los dispositivos móviles se han convertido en instrumentos de uso cotidiano. Se utilizan para comunicarse, navegar por internet, acceder a servicios bancarios, redes sociales, gestionar agendas, gestionar consultas médicas y trámites con las Administraciones Públicas, etc. Gracias a su disponibilidad prácticamente continua, se han convertido en 'almacenes' de datos y fotografías o vídeos, algunos de los cuales pueden ser considerados datos personales. Estas incuestionables ventajas en facilidad de uso y comodidad vienen acompañadas por unos riesgos de los cuales en muchas ocasiones los usuarios no son plenamente conscientes.

En nuestra opinión esto tiene relación con el proceso de instalación. Cuando un usuario instala una aplicación, se le presenta una lista de los permisos a los que accederá la aplicación, pero no se le informa de modo claro y sencillo sobre el alcance del permiso, el tipo de datos al que accede y los problemas de privacidad asociados a ese permiso. Para conseguir esta información debería consultar la política de privacidad asociada a la aplicación. Surge así la cuestión sobre cómo empoderar a los usuarios, hacerles conscientes de su nivel de exposición, de los riesgos que esta exposición conlleva, y de qué acciones pueden tomar para reducir esta exposición y riesgos.

El Reglamento General de Protección de Datos, RGPD [1] y la Ley Orgánica 3/2018, LOPD-GDD [2] exigen que las políticas de privacidad informen adecuadamente sobre los datos personales que cada aplicación recoge, con qué fin y con quién los comparte. El problema es que estas políticas de privacidad son textos en formato libre, largos, con varias páginas, de difícil lectura incluso para usuarios con un nivel cultural alto, obviamente mucho más difíciles de entender para colectivos desfavorecidos en este aspecto: menores que no han alcanzado la madurez intelectual, personas con capacidades intelectuales reducidas por cuestiones de educación o de salud, u otros. Incluso los colectivos no desfavorecidos reconocen no leer las políticas de privacidad en la mayoría de las ocasiones, encontrarlas difícilmente comprensibles[1] [3].

En el proyecto App-PI (*App Privacy Impact*) partimos de la hipótesis de que si los usuarios disponen de herramientas fáciles de entender y fáciles de utilizar, les resulta mucho más fácil empoderarse en la protección de su privacidad cuando utilizan sus dispositivos móviles. Para ayudar en esta tarea, diseñamos un ecosistema donde los usuarios interaccionan con servicios que ofrecen en formatos amigables los resultados de indicadores de privacidad. Estos indicadores utilizan a su vez como datos para sus cálculos los metadatos recopilados y almacenados en un repositorio de metadatos. Acercar el control sobre su privacidad a los usuarios finales ha guiado el diseño de todos y cada uno de estos elementos. De este modo, el repositorio almacena metadatos que no se encuentran en otros repositorios similares, la métrica trabaja con los grupos de permisos, que es lo que los usuarios finales pueden traducir en algo manejable en sus dispositivos, y las aplicaciones de usuario utilizan interfaces, iconos y tipos de diagramas sencillos y conocidos, de muy fácil comprensión para cualquier perfil de usuario.

En la sección II revisamos el trabajo realizado en el campo de la privacidad móvil en los tres aspectos que nos interesan: servicios para usuarios, métricas para privacidad y repositorios de metadatos. En la sección III presentamos el ecosistema, el repositorio y la métrica que actualmente estamos utilizando. La sección IV cierra este artículo con las conclusiones más importantes obtenidas hasta el momento.

[1] https://www.tosdr.org/

II. La gestión de la privacidad de los usuarios de aplicaciones móviles

II-A. *Servicios para informar a los usuarios*

Existen servicios de usuario, disponibles en la web, que ofrecen información sobre riesgos para la privacidad cuando se utilizan servicios digitales en la web. Algunos reconocidos son *Privacy Score*[2] y *Terms of Service Didn't Read (ToS;DR)*[3]. Aunque no se trata de servicios especializados en aplicaciones móviles (*apps*), merece la pena prestarles atención. Utilizar un servicio accesible en un navegador tiene la ventaja de su accesibilidad, ya que no requiere la instalación de software adicional. Pero sobre todo la ventaja de minimizar los riesgos para los derechos y libertades de sus usuarios relativos a la protección de sus datos personales, puesto que no se ven obligados a exponer sus dispositivos, ni tampoco sus datos personales para hacer una consulta. Son servicios cuyo uso no requiere registrarse.

Existen otros servicios, específicos para los usuarios de aplicaciones móviles. Es el caso de *Exodus Privacy*[4] o *Privacy Grade*[5][4]. Estos servicios presentan a sus usuarios una recopilación de los permisos que declaran las aplicaciones y datos a los que acceden, proporcionando datos verídicos y fiables. En nuestra opinión, el problema es que esta información es difícilmente comprensibles para los usuarios sin conocimientos avanzados en tecnología, quienes no conocen el detalle de los permisos del sistema Android, su significado o relevancia [5]. En consecuencia, no saben cómo utilizar esta información sobre los permisos para configurar sus dispositivos para proteger mejor su privacidad.

Lo que los usuarios pueden controlar en los Ajustes de sus dispositivos no son los *permisos*, sino los *grupos de permisos*. En consecuencia, una persona nunca podrá encontrar en su dispositivo el modo de conceder o denegar permisos como *android.permission.SYSTEM_CAMERA* o *android.permission.CAMERA*. Lo que verá será un "permiso" de *Cámara*, que podrá conceder o denegar. En realidad se trata de un grupo de permisos, dentro del cual se encuentran los dos permisos indicados, tal como se puede apreciar en la figura 1, que muestra una captura de pantalla de los Ajustes de un dispositivo Android. Los usuarios conceden o deniegan grupos de permisos en bloque, nunca permisos individuales. En nuestra opinión, esto hace que no sepan cómo utilizar información relativa a permisos individuales.

Son varios los sistemas operativos de teléfonos móviles, pero los tres principales son: Android, iOS y Windows Phone. Android, desarrollado por Google, es el sistema operativo que abarca tres cuartos de la cuota de mercado mundial, con más de tres billones de usuarios, en 190 países[6]. Por ello, este trabajo se centra en las aplicaciones Android. En este artículo se propone una solución similar a las que analizan la privacidad en sitios web, por ej., *PrivacyScore* [6], pero aplicado a aplicaciones móviles en sistemas Android.

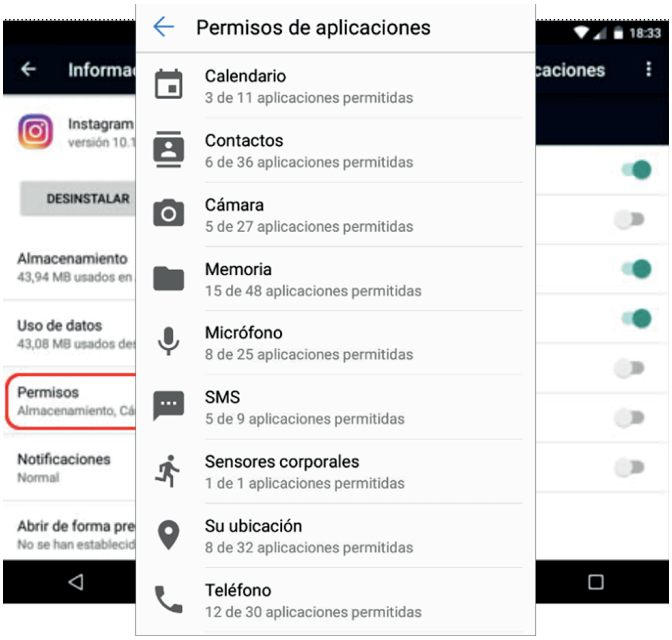

Figura 1. Grupos de permisos en un dispositivo Android.

II-B. *Métricas de privacidad*

Se han propuesto varias métricas que utilizan datos sobre los permisos que requieren las aplicaciones móviles [7], [8], [9], [10], [11]. Sin embargo, son métricas cuyo objetivo es la detección de *malware*. No son métricas diseñadas para medir el riesgo para su privacidad que asumen los usuarios de las aplicaciones móviles. Aunque hay propuestas que analizan el impacto sobre la privacidad de las *apps* [12], [13], [14], no incluyen métricas que ofrezcan a los usuarios finales indicadores fácilmente comprensibles.

II-C. *Repositorios y servicios de metadatos*

En la actualidad existen algunos almacenes de aplicaciones móviles [15]. Entre los más voluminosos en número de aplicaciones se encuentran *AndroZoo* [16] y el de *AndroVault* [17]. El primero almacena los archivos *.apk*, mientras que el segundo se centra en la extracción de conocimiento de aplicaciones por medio de diversos análisis. Aunque almacenan una gran cantidad de aplicaciones, no hay metadatos relativos a la privacidad y seguridad de las aplicaciones.

En el caso de *AndroZoo*, en diciembre de 2023 se ha añadido la extracción de metadatos de *Google Play*[7]. No obstante, estos metadatos no incluyen los grupos de permisos, posibles puntuaciones de privacidad, o la naturaleza estructurada de algunos de los metadatos como los AOSP (*Android Open Source Project*). Todos ellos datos que pueden ayudar a construir herramientas para empoderar a los usuarios en la protección de su privacidad.

Si nos centramos en repositorios y servicios orientados a la privacidad, merece la pena resaltar *Exodus Privacy*[8] y *Privacy Grade*[9][4], si bien este último ya no está activo. *Exodus Privacy* ofrece un repositorio donde se puede obtener la lista de permisos que las *apps* solicitan y los *trackers* que

[2]https://privacyscore.org/
[3]https://tosdr.org/
[4]https://exodus-privacy.eu.org/
[5]https://android-network-tracing.herokuapp.com/privacygrade
[6]Fuente: Android Statistics (2024). https://www.businessofapps.com/data/android-statistics/
[7]https://play.google.com/store/apps
[8]https://exodus-privacy.eu.org/
[9]https://android-network-tracing.herokuapp.com/privacygrade

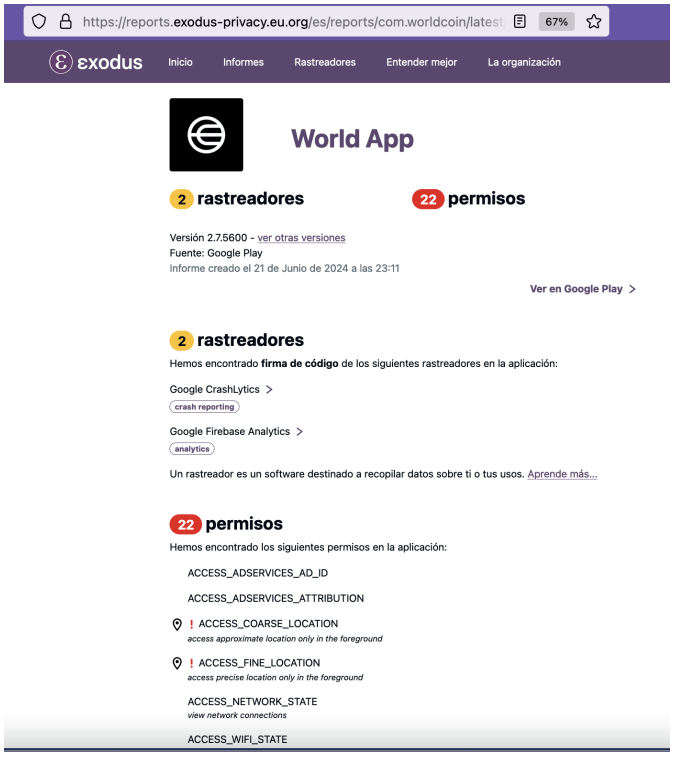

Figura 2. Resultados para la app *World App* en *Exodus Privacy*.

utilizan [14]. También ofrece un servicio online donde es posible visualizar estos resultados. La figura 2 muestra una captura de los resultados para la app *World App*. Se pueden ver el número total de rastreadores (*trackers*) y el número total de permisos, 22, seguido de un listado de los rastreadores encontrados y los permisos. Marca cada permiso con un icono en función de su peligrosidad. Al igual que ocurre con *AndroZoo*, nuestra experiencia en actividades formativas y de divulgación, nos indica que los usuarios finales no comprenden el significado de una lista de permisos extensa[10] ni son capaces de discriminar sobre cuáles pueden actuar, o aquellos que tienen mayor impacto sobre su privacidad. En realidad, lo que cualquier usuario/a puede manejar desde los Ajustes de su dispositivo son grupos de permisos. Coloquialmente conocidos como ”permisos”, aunque Android diferencia entre *permisos* y *grupos de permisos*.

III. El ecosistema App-PI: ciudadanía, móviles y privacidad

III-A. Arquitectura al servicio de la calidad y la autoprotección

Nuestra propuesta es *App Privacy Impact* (App-PI), un ecosistema para la evaluación del impacto de *apps* para dispositivos móviles sobre la privacidad y seguridad de sus usuarios. Este ecosistema consta de los elementos que se pueden ver en la figura 3. Son:

- Repositorio App-PIMD (*App Privacy Impact MetaData*) y los procesos ETL[11] asociados: un almacén de metadatos de aplicaciones Android. Los metadatos se utilizan para calcular el impacto en la privacidad de los usuarios [18].
- API[12]: un acceso abierto de los contenidos del repositorio para otros servicios e investigadores [18].
- Métricas que calculen el impacto de las aplicaciones en la privacidad de los usuarios haciendo uso de la información del *warehouse*. Actualmente está en funcionamiento la métrica App-PIM, que se presenta en la sección III-C.
- Aplicaciones para usuarios finales que implementan las métricas y ofrecen servicios de usuario [19]. El servicio que actualmente está en funcionamiento es *APK Falcon*, que también se presenta en la sección III-C.

[10] Algunas aplicaciones móviles llegan a solicitar más de 80 permisos.
[11] ETL: *Extract, Transform, Load*.

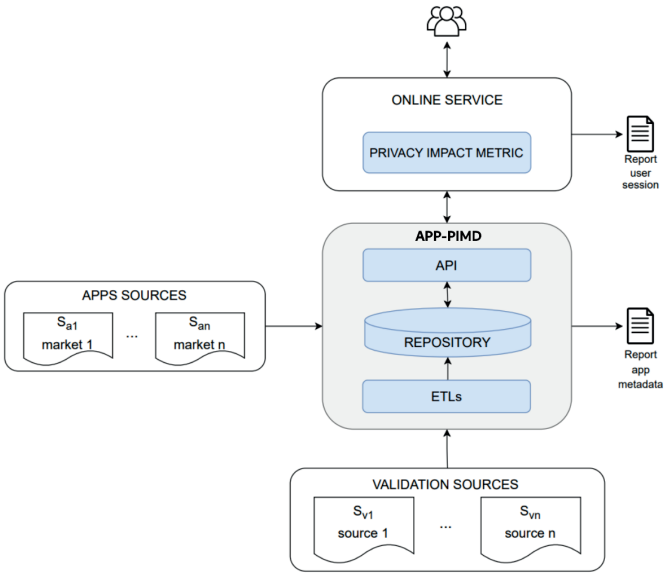

Figura 3. Arquitectura de App-PI.

III-B. El repositorio App-PIMD y los metadatos que la ciudadanía puede aprovechar

El repositorio App-PIMD se diseñó como un servicio de consulta para servicios que realizan análisis para conocer el impacto sobre la privacidad y seguridad de los usuarios. Estos servicios pueden ser internos, desarrollados por el equipo de investigación que mantiene el repositorio, o externos. Para poblar App-PIMD se recopilan metadatos, acorde a un modelo de *warehousing*. Estos datos se pueden consultar utilizando una API (ver Fig. 3), la cual reenvía las consultas a la base de datos MySQL donde se almacenan. Se decidió no ofrecer acceso directo con consultas SQL por seguridad. Para garantizar la calidad de sus datos, se decidió trabajar con tres perfiles para el acceso a sus datos:

- **General**, el tipo de usuario más frecuente. No es necesario estar registrado para acceder con este perfil. Este tipo de usuario puede consultar los contenidos del *warehouse*. También puede solicitar la carga de nuevas aplicaciones para enriquecerlo.
- **Experto/a** en puntuar el nivel de intromisión de aplicaciones móviles. La diferencia sustancial con el perfil anterior es que puede modificar el contenido (nunca los esquemas) del *warehouse*. Es necesario registrarse para acceder con este perfil.

[12] API: *Application Programming Inteface*.

- **De administración**. Este perfil se encarga de actualizar directamente el *warehouse*, así como asegurar la calidad de los datos del mismo, por ejemplo, llevando a cabo la carga masiva de aplicaciones. Está reservado para el grupo de investigación que mantiene el *warehouse*.

Los metadatos que se almacenan recogen las propiedades características de las aplicaciones móviles, tal como las han definido sus desarrolladores, independientemente del dispositivo en el que se instala, principalmente los datos disponibles en los ficheros *AndroidManifest.xml*. Las fuentes de datos utilizadas para conseguir estos ficheros son repositorios con un prestigio reconocido como fuentes de confianza, tales como *AndroZoo*, del cual se ha hablado en la sección II. De cada aplicación se almacenan metadatos identificativos de la misma como su nombre de paquete, su *hash* SHA256, su versión, su categoría y metadatos sobre su extracción como la fuente y fecha entre otros. En referencia a los metadatos relacionados con la intromisión en la privacidad se almacenan los permisos que esta utiliza, los grupos de permisos, así como las puntuaciones de intromisión obtenidas por la aplicación cuando se le aplican métricas de privacidad.

En el *warehouse* se almacena también información complementaria, sobre el sistema operativo Android. Las fuentes de los metadatos de Android y su sistema de permisos son las páginas web HTML de documentación [13] y código del sistema Android [14]. Entre esta información se incluyen los permisos y grupos de permisos que declara el sistema operativo Android (ejemplo de permiso: *android.permission.READ_SMS*). Para cada permiso se almacena su nivel de protección o tipo, su identificador o nombre, en qué versión del sistema se incluyó, así como el grupo de permisos al que pertenece. Además, de cada permiso de tipo *dangerous* se almacena una puntuación sobre el impacto en la privacidad que este tiene [20]. También se recogen los datos sobre la seguridad de los datos que Google incorpora en su *market*[15] para informar a sus usuarios sobre la seguridad y privacidad de sus datos en las aplicaciones [21].

Las fuentes de datos de las cuales se recoge el nivel de intromisión en la privacidad de las aplicaciones son ToS;DR [22] y los datos obtenidos por otros investigadores en este campo [23], [24]. Cada valor se normaliza para obtener un valor cuantitativo que se pueda comparar con los demás. De este modo se facilita la comparación de las puntuaciones obtenidas por una misma app por diferentes servicios de evaluación.

III-C. Indicadores de privacidad para una ciudadanía autoprotegida

Actualmente ofrecemos un indicador consistente en una métrica basada en los permisos, y grupos de permisos, declarados por los desarrolladores de las *apps* en el fichero *AndroidManifest.xml*. También utiliza información sobre la explotación de estos permisos por el *malware*. Se considera que suponen mayor riesgo para la privacidad aquellos permisos que han sido más explotados por el *malware*. Todos estos datos están almacenados en el repositorio App-PIMD. Se basa en las siguientes premisas:

- Los únicos permisos que los usuarios pueden conceder son los permisos de tipo *dangerous* [25].
- Los grupos de permisos están formados por permisos de tipo *dangerous* [25].
- El *malware* tiende a pedir más permisos que las aplicaciones benignas y usar un mayor número de permisos que éstas [13], [26].

Teniendo en cuenta las premisas anteriores, se propone una métrica, App-PIM (*App Privacy Impact Metric*), cuya fórmula se muestra en la *Ec. (1)*. App-PIM relaciona de forma cuantitativa los permisos de tipo *dangerous* con los grupos de permisos. Esta aproximación, novedosa respecto a los restantes servicios comentados en la sección II-A, permitirá a los usuarios conocer cómo varía el impacto de las *apps* en su privacidad al activar o desactivar los grupos de permisos en los Ajustes de sus dispositivos. Se ha buscado un indicador sencillo, fácil de entender, por lo cual la fórmula no toma en consideración la legitimidad del uso de los permisos. En realidad, la legitimidad se corresponde con el uso de los datos, no de los permisos. Pero, como ya hemos avanzado en publicaciones anteriores, la escasa granularidad del sistema de permisos Android no permite hacer una asociación directa dato-permiso, razón por la cual se ha preferido trabajar con datos objetivos y neutros. Sin embargo, se ha buscado que los usuarios puedan relacionar fácilmente los resultados que les ofrecemos con la información que pueden obtener en *Google Play* acerca del uso de los datos (información sobre Seguridad de los Datos). Si en esa información se informa de que un permiso se solicita para acceder a un dato de forma legítima, cada usuario o usuaria podrá decidir libremente qué acción realizar. La fórmula de App-PIM trabaja con:

$$M(app) = \frac{\sum_{i=1}^{n}(e_i \sum_{j=1}^{m} p_{ij})}{max_I} \quad (1)$$

- app: aplicación de la que se quiere obtener el valor del impacto sobre la privacidad de los usuarios.
- $M(app)$: valor del impacto sobre la privacidad de la aplicación app. El valor devuelto por $M(app)$ está comprendido entre 0 y 1, es decir, $M(app) \in [0, 1]$.
- n: número de grupos de permisos utilizados por la aplicación app.
- e_i: estado del grupo de permisos $i-ésimo \in \{0, 1\}$. 0 indica que el grupo de permisos $i-ésimo$ está inactivo; 1 indica que el grupo de permisos $i-ésimo$ está activo.
- m: para cada grupo de permisos, número de permisos utilizados por la aplicación app.
- p_{ij}: peso del permiso $j_ésimo$ dentro del grupo de permisos $i_ésimo$ utilizado por la aplicación app. Los pesos p_{ij} se asignan con las puntuaciones del *ranking* utilizado en [27], [28]. Los situados en las posiciones más altas del ranking se consideran más intrusivos, esto es, tienen mayor peso. En el caso de que el permiso no esté en el *ranking*, el peso asignado a estos permisos es menor que cualquier peso asignado a permisos presentes en el *ranking* de permisos explotados por el *malware*.
- max_I: impacto máximo, el de una aplicación que acceda a todos los grupos de permisos disponibles.

[13] https://developer.android.com/
[14] https://android.googlesource.com/
[15] https://play.google.com/store/apps

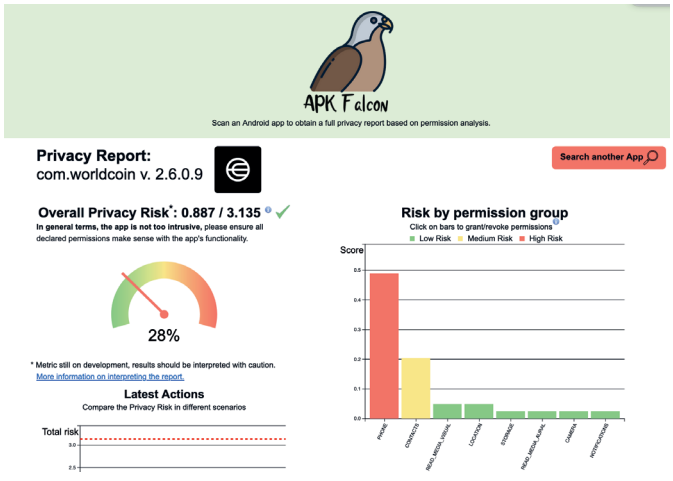

Figura 4. Resultados para la app *World App* en *APK Falcon*.

Para facilitar la utilización de este indicador, se proporciona una aplicación online, *APK Falcon*[16]. Los resultados de aplicar la métrica a la app *World Coin* se muestran en la figura 4. En el numerador el valor es 1, 0.887, y en el denominador el valor de max_I, 3.135. En el panel izquierdo se muestra el resultado cuantitativo obtenido, un 28 % en este caso, lo cual da una idea general del impacto de una app sobre la privacidad de sus usuarios (el porcentaje se calcula con respecto a una aplicación que solicitase todos los permisos posibles). En el panel derecho se muestra el peso que cada uno de los grupos de permisos tiene sobre este impacto. El valor añadido en usabilidad es que los usuarios pueden realizar simulaciones para saber cómo variaría este impacto cuando conceden o deniegan uno de estos ”permisos” (grupos de permisos): clickando sobre la barra correspondiente *conceden* o *deniegan* ese grupo de permisos.

III-D. Aceptación por parte de los usuarios finales

Se están realizando talleres con usuarios finales, en los que se ha utilizado *APK Falcon* y la métrica presentada. Los perfiles son heterogéneos, tanto en edad, como en nivel de formación y competencias digitales. Hasta ahora se han realizado cuatro talleres, en los cuales han participado un total de 90 personas, incluyendo estudiantes con edades inferiores a 30 años, y también personas cuyas edades superan 60 años. Aunque se está trabajando en el análisis de los resultados, los primeros resultados apuntan que la aceptación es razonablemente buena. La figura 5 muestra los resultados de la pregunta sobre la facilidad de uso de la herramienta *APK Falcon*. Dos tercios de los usuarios consideran fácil de utilizar la herramienta. Los dos aspectos mejor valorados en estos talleres han sido la sencillez del indicador y la posibilidad de asociar rápidamente los resultados visualizados con su capacidad de acción en los Ajustes de sus dispositivos. En segundo lugar, la posibilidad de utilizar el servicio sin registrarse ni aportar ningún dato personal. Entre las demandas recibidas, la más numerosa es la disponibilidad de una versión en forma de *app*, formato sobre el cual trabajaremos próximamente.

[16]El código que implementa la métrica está disponible en el repositorio https://gitlab.inf.uva.es/javcres/uva-apk-falcon, junto con la documentación de diseño.

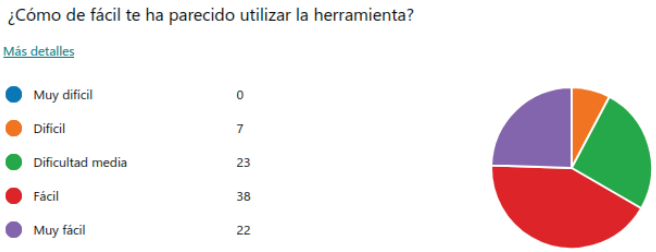

Figura 5. Resultados de las encuestas en un taller con usuarios finales.

IV. Conclusiones

App-PI aporta instrumentos para satisfacer el Objetivo 9. *Industria, Innovación e Infraestructura* de la Agenda 2030[17], contribuyendo a “Capacitar a las personas con la ayuda de una nueva generación de tecnologías”. En este ecosistema se ofrece un conjunto de herramientas para que los usuarios de aplicaciones móviles (*apps*) comprendan fácilmente el impacto que tienen éstas en su privacidad y puedan actuar para proteger sus datos personales de una manera eficaz. Se consigue a través de varios aspectos clave: una interacción sencilla, apoyada por instrumentos gráficos, el recurso del aprendizaje basado en simulaciones, y sobre todo, la utilización de conceptos que los usuarios utilizan en sus propios dispositivos. Además, se ofrece a otros grupos de investigación y desarrolladores trabajando en este campo un repositorio de metadatos para que puedan construir sus propias herramientas de usuario final. Hasta donde conocemos, existen otros sistemas donde se ofrecen herramientas similares, pero ninguno donde todo ello se combine como se hace en este ecosistema. Destacamos algunas aportaciones:

1. La métrica *App-PIM* se basa en conceptos con los que los usuarios de aplicaciones móviles están familiarizados. Aunque existen otras métricas de privacidad, no se han adaptado a los grupos de permisos, que es lo que en realidad pueden manejar los usuarios en los ajustes de sus dispositivos.
2. El servicio de usuario *APK Falcon* ofrece interfaces gráficas, fáciles de manejar, particularmente adaptadas a colectivos a los que resulta difícil comprender las políticas de privacidad. Estas herramientas permiten aprender y entender “haciendo”, esto es, “jugando” sin asumir riesgos en sus dispositivos personales. Hasta donde conocemos, no existen propuestas con estas características.
3. Se ha aplicado la privacidad desde el diseño: *APK Falcon* es un servicio disponible en la web, de uso libre. No es necesario registrarse ni exponer datos personales. Entendemos que esto es particularmente útil para grupos especialmente expuestos como menores, personas con discapacidad o personas en situaciones vulnerables que necesitan servicios en los cuales no pongan en riesgo sus datos personales.
4. Asimismo, la seguridad se ha tenido en cuenta en el diseño del repositorio App-PIMD: el uso de una API, perfiles diferenciados, y otras medidas de seguridad expuestas en [29] ayudan a alcanzar la seguridad deseada.

[17]https://www.un.org/sustainabledevelopment/es/infrastructure/

Como trabajo futuro se prevén ampliaciones y adaptaciones en función de las opiniones recogidas en los talleres formativos. También se contempla la propuesta de nuevas métricas donde se utilizarán metadatos sobre la Seguridad de los Datos que los desarrolladores ofrecen en *Google Play*.

AGRADECIMIENTOS

Este trabajo se incluye en las actividades del proyecto estratégico de ciberseguridad "App-PI (*App Privacy Impact*): Un ecosistema para la evaluación del impacto de *apps* para dispositivos móviles sobre la privacidad y seguridad de sus usuarios", el cual se realiza al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation), el proyecto del Gobierno de España que traza la hoja de ruta para la modernización de la economía española, la recuperación del crecimiento económico y la creación de empleo, para la reconstrucción económica sólida, inclusiva y resiliente tras la crisis de la COVID19, y para responder a los retos de la próxima década.

REFERENCIAS

[1] D. Diario Oficial de la Unión Europea, "Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos)," ELI: http://data.europa.eu/eli/reg/2016/679/oj, 4 de mayo 2016.

[2] p. . a. . Boletín Oficial de Estado (BOE) núm. 294, de 6 de diciembre de 2018, "Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales," ELI: https://www.boe.es/eli/es/lo/2018/12/05/3, 2018, eLI: https://www.boe.es/eli/es/lo/2018/12/05/3.

[3] V. Bracamonte, S. Hidano, W. B. Tesfay, and S. Kiyomoto, "User study of the effectiveness of a privacy policy summarization tool," in *Information Systems Security and Privacy*, P. Mori, S. Furnell, and O. Camp, Eds. Cham: Springer International Publishing, 2020, pp. 186–206.

[4] H. Jin, M. Liu, K. Dodhia, Y. Li, G. Srivastava, M. Fredrikson, Y. Agarwal, and J. I. Hong, "Why are they collecting my data?: Inferring the purposes of network traffic in mobile apps," *Proc. ACM Interact. Mob. Wearable Ubiquitous Technol.*, vol. 2, no. 4, pp. 173:1–173:27, 2018. [Online]. Available: https://doi.org/10.1145/3287051

[5] A. Mathur, E. Ewoldt, Q. Niyaz, A. Y. Javaid, and X. Yang, "Permission-educator: App for educating users about android permissions," in *Intelligent Human Computer Interaction - 13th International Conference, IHCI 2021, Kent, OH, USA, December 20-22, 2021, Revised Selected Papers*, ser. Lecture Notes in Computer Science, J. Kim, M. Singh, J. Khan, U. S. Tiwary, M. Sur, and D. Singh, Eds., vol. 13184. Springer, 2021, pp. 361–371. [Online]. Available: https://doi.org/10.1007/978-3-030-98404-5_34

[6] M. contributors. (2017) Privacyscore. [Online]. Available: https://privacyscore.org/

[7] Y. Bai, S. Chen, Z. Xing, and X. Li, "Argusdroid: detecting android malware variants by mining permission-api knowledge graph," *Sci. China Inf. Sci.*, vol. 66, no. 9, 2023. [Online]. Available: https://doi.org/10.1007/s11432-021-3414-7

[8] M. Cristiá, G. D. Luca, and C. Luna, "An automatically verified prototype of the android permissions system," *J. Autom. Reason.*, vol. 67, no. 2, p. 17, 2023. [Online]. Available: https://doi.org/10.1007/s10817-023-09666-2

[9] A. Ehsan, C. Catal, and A. Mishra, "Detecting malware by analyzing app permissions on android platform: A systematic literature review," *Sensors*, vol. 22, no. 20, p. 7928, 2022. [Online]. Available: https://doi.org/10.3390/s22207928

[10] M. Shah, "Detecting over-claim permissions and recognising dangerous permission in android apps," *Int. J. Inf. Comput. Secur.*, vol. 17, no. 1/2, pp. 204–218, 2022. [Online]. Available: https://doi.org/10.1504/IJICS.2022.121298

[11] H. Wang, W. Zhang, and H. He, "You are what the permissions told me! android malware detection based on hybrid tactics," *J. Inf. Secur. Appl.*, vol. 66, p. 103159, 2022. [Online]. Available: https://doi.org/10.1016/j.jisa.2022.103159

[12] J. Gamba, M. Rashed, A. Razaghpanah, J. Tapiador, and N. Vallina-Rodriguez, "An analysis of pre-installed android software," in *2020 IEEE Symposium on Security and Privacy, SP 2020, San Francisco, CA, USA, May 18-21, 2020*. IEEE, 2020, pp. 1039–1055. [Online]. Available: https://doi.org/10.1109/SP40000.2020.00013

[13] Á. Feal, P. Calciati, N. Vallina-Rodriguez, C. Troncoso, A. Gorla *et al.*, "Angel or devil? a privacy study of mobile parental control apps," *Proceedings of Privacy Enhancing Technologies (PoPETS)*, vol. 2020, 2020.

[14] P. Laperdrix, N. Mehanna, A. Durey, and W. Rudametkin, "The price to play: A privacy analysis of free and paid games in the android ecosystem," in *WWW '22: The ACM Web Conference 2022, Virtual Event, Lyon, France, April 25 - 29, 2022*, F. Laforest, R. Troncy, E. Simperl, D. Agarwal, A. Gionis, I. Herman, and L. Médini, Eds. ACM, 2022, pp. 3440–3449. [Online]. Available: https://doi.org/10.1145/3485447.3512279

[15] F.-X. Geiger and I. Malavolta, "Datasets of Android Applications: a Literature Review," *ArXiv*, vol. abs/1809.10069, 2018. [Online]. Available: https://api.semanticscholar.org/CorpusID:52845379

[16] K. Allix, T. F. Bissyandé, J. Klein, and Y. Le Traon, "AndroZoo: Collecting Millions of Android Apps for the Research Community," in *Proceedings of the 13th International Conference on Mining Software Repositories*, 2016, pp. 468–471.

[17] G. Meng, Y. Xue, J. K. Siow, T. Su, A. Narayanan, and Y. Liu, "AndroVault: Constructing Knowledge Graph from Millions of Android Apps for Automated Analysis," *ArXiv*, vol. abs/1711.07451, 2017. [Online]. Available: https://api.semanticscholar.org/CorpusID:1736293

[18] A. Pérez-Fuente, "Data Warehouse para el estudio de la privacidad de aplicaciones móviles," Trabajo fin de Grado, Universidad de Valladolid, 2023.

[19] J. Crespo Guerrero, "APKFalcon: Servicio de usuarios para la evaluación y comprensión del impacto sobre la privacidad de aplicaciones móviles," Trabajo fin de Grado, Universidad de Valladolid, 2023.

[20] M. Upadhayay, A. Sharma, G. Garg, and A. Arora, "RPNDroid: Android Malware Detection using Ranked Permissions and Network Traffic," in *2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4)*, 2021, pp. 19–24.

[21] Android Developers. (2021) Declara el uso de datos de tu app. [Online]. Available: https://developer.android.com/privacy-and-security/declare-data-use?hl=es-419

[22] H. Roy. (2012) Terms of Service Didn't Read. [Online]. Available: https://tosdr.org/

[23] M. Hatamian, N. Momen, L. Fritsch, and K. Rannenberg, "A Multilateral Privacy Impact Analysis Method for Android Apps," in *Privacy Technologies and Policy*, M. Naldi, G. F. Italiano, K. Rannenberg, M. Medina, and A. Bourka, Eds., 2019, pp. 87–106.

[24] S. Barth, M. de Jong, M. Junger, P. H. Hartel, and J. C. Roppelt, "Putting the privacy paradox to the test: Online privacy and security behaviors among users with technical knowledge, privacy awareness, and financial resources," in *Telematics Informatics*, vol. 41, 2019, pp. 55–69.

[25] A. Aparicio, M. M. Martínez-González, and V. Cardeñoso, "Métrica basada en grupos de permisos para entender el impacto de las aplicaciones android sobre la privacidad," in *2022 17th Iberian Conference on Information Systems and Technologies (CISTI)*, 2022, pp. 1–5.

[26] P. Calciati, "Understanding the evolution of android applications," Ph.D. dissertation, ETSI_Informatica, 2019.

[27] V. P. Dharmalingam and V. Palanisamy, "A novel permission ranking system for android malware detection—the permission grader," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, pp. 5071–5081, 2021.

[28] Y. Wang, J. Zheng, C. Sun, and S. Mukkamala, "Quantitative security risk assessment of android permissions and applications," in *Database Security*, 2013.

[29] A. Pérez-Fuente, M. Mercedes Martínez-González, A. Aparicio, and Q. Moro, "Un Data Warehousse para el Estudio de la Privacidad y Seguridad de Aplicaciones Móviles," in *Actas de las IX Jornadas Nacionales de Investigación en Ciberseguridad (JNIC 2024)*, ser. Jornadas Nacionales de Investigación en Ciberseguridad (JNIC), A. M. R. Quintero, R. C. Guerrero, and Ángel J. Varela Vaca, Eds., vol. 3531. Universidad de Sevilla, 2024, pp. 624–631. [Online]. Available: https://idus.us.es/handle/11441/159179