Mi Privacidad y mis dispositivos móviles: ¿cómo tomar el control y autoprotegerme?

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).

INGPRIV
GRUPO DE INVESTIGACIÓN EN INGENIERÍA DE LA PRIVACIDAD

El proyecto App-PI es una iniciativa realizada 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)

Mi Privacidad y mis dispositivos móviles: ¿cómo tomar el control y autoprotegerme?

Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid

Universidad de Valladolid

gi.ingpriv@uva.es

Autores:

M. Mercedes Martínez González, Amador Aparicio de la Fuente, Alejandro Pérez de la Fuente, Margarita Gonzalo Tasis, Quiliano Isaac Moro Sancho

Colaboradores:

Iván Martín Colomo, Génesis Michel de León Alcántara, Mónica Melero Lázaro, Luis Blanco de la Cruz

El proyecto App-PI es una iniciativa realizada 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)

Tabla de contenido

El proyecto APP-PI es una iniciativa realizada 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 APP-PI es una iniciativa realizada 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)

MÓDULO 1:

LA PRIVACIDAD

Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[1]

Universidad de Valladolid

gi.ingpriv@uva.es

[1]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz y Génesis M. De León Alcántara.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

En el mundo actual, la privacidad es un derecho esencial que nos permite proteger nuestra información personal y decidir quién puede acceder a ella. Antes, estaba más relacionada con la intimidad física, pero ahora también abarca el entorno digital, donde constantemente compartimos datos a través de dispositivos y plataformas. Para responder a este cambio, han surgido leyes diseñadas para protegernos frente a las amenazas digitales. En este módulo hablaremos sobre cómo ha evolucionado la privacidad, por qué es clave para nuestra seguridad y libertad y cómo las normativas influyen en un mundo cada vez más conectado.

1. ¿Qué entendemos por privacidad?

El concepto de privacidad se puede definir como "Ámbito de la vida privada que se tiene derecho a proteger de cualquier intromisión"[2].

La privacidad trata de controlar y proteger nuestra información personal, así como decidir qué compartimos y con quién lo hacemos. No se limita únicamente a información que proporcionamos de forma consciente; también incluye todos los datos generados durante nuestra vida cotidiana (como nuestra residencia, intereses personales, etc.), abarcando todas las áreas donde tenemos derecho a mantener los detalles de nuestra vida personal fuera del alcance público o de entidades comerciales para proteger nuestra dignidad, seguridad y libertad.

¿Sabías qué…?

En nuestro país, la privacidad está vinculada al derecho a la intimidad, que aparece recogido en el artículo 18 de la Constitución Española.

Por ello, es un **derecho fundamental** que, en el mundo actual, abarca diferentes aspectos.

[2]Definición de privacidad según la RAE: https://dle.rae.es/privacidad

El proyecto APP-PI es una iniciativa realizada 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)

2. La privacidad en el mundo actual

Antes, la privacidad se asociaba con la protección de un espacio íntimo, libre de observación o control externo. Ahora, con las nuevas tecnologías integradas en nuestra vida diaria, surgen nuevas formas en las que nuestra privacidad puede verse comprometida. Por eso, este concepto se ha ampliado y adaptado al entorno digital, donde generamos y compartimos información de manera constante a través de dispositivos y plataformas.

Para entender mejor el alcance de la privacidad en nuestra sociedad, podemos fijarnos en los distintos aspectos de nuestra vida en los que podemos hablar de privacidad:

- **Privacidad física**: Es el enfoque más tradicional. Está relacionada con el espacio personal y el derecho a no ser observado ni registrado sin consentimiento. Sigue siendo especialmente relevante hoy en día. Por ejemplo, la videovigilancia está cada vez más presente en espacios públicos.

- **Privacidad de la información**: Se refiere al derecho de cada individuo a mantener el control sobre sus datos personales, como su nombre, dirección, historial de navegación, contactos y demás información sensible. Es especialmente importante en el entorno digital, donde las empresas manejan grandes cantidades de información que aportamos para que puedan darnos los servicios que contratamos.

El proyecto APP-PI es una iniciativa realizada 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)

- **Privacidad de la comunicación**: Se centra en la protección de nuestras conversaciones y comunicaciones, ya sea en llamadas, mensajes de texto, correos electrónicos o aplicaciones de mensajería. Implica garantizar que nuestras comunicaciones no sean vigiladas ni interceptadas sin nuestra autorización. En el mundo digital se refiere a proteger nuestras comunicaciones por correo electrónico, redes sociales, o cualquier otro medio que podamos utilizar para comunicarnos con otras personas.

- **Privacidad de la ubicación**: Consiste en controlar quién y cuándo puede acceder a nuestra ubicación geográfica. Los servicios de geolocalización se han convertido en algo habitual en aplicaciones y dispositivos. Es fundamental proteger esta información para evitar que se use o comparta sin nuestro conocimiento.

Como vemos, existen numerosas situaciones en las que nuestra privacidad se puede ver vulnerada. Los puntos que se han comentado **ponen de manifiesto la importancia de proteger nuestra privacidad**, que se puede resumir en dos razones:

1. **No discriminación:** existen datos como nuestra raza, sexo, religión, afiliación política, orientación sexual, etc., que **podrían ser utilizados de forma discriminatoria.**

2. **Libertad y autonomía:** la privacidad nos permite actuar de manera libre y autónoma sin temor a ser vigilados. Sin este derecho, **podríamos sentirnos coaccionados a comportarnos de cierta manera o a no expresar opiniones en público**.

Teniendo esto en cuenta, y habiendo visto que la privacidad emana de un derecho reconocido en nuestra Constitución, surgen las siguientes preguntas: ¿qué dice la legislación actual al respecto? Y ¿estamos adecuadamente protegidos?

3. La privacidad en la legislación actual

Para proteger la privacidad de los ciudadanos en entornos digitales, la Unión Europea (UE) fue puntera promoviendo la normativa que ha servido de referencia para avanzar en la protección de nuestra privacidad, el **Reglamento General de Protección de Datos**

El proyecto APP-PI es una iniciativa realizada 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)

(RGPD). Esta norma es de 2016. En España se proyecta sobre la **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**, que desde 2018 recoge sus mandatos y los extiende con algunos adicionales relativos a nuestros derechos digitales.

3.1. El Reglamento general de protección de datos (RGPD)

El **Reglamento General de Protección de Datos (RGPD)**[3] es la legislación europea que regula los derechos de los ciudadanos sobre sus datos personales y establece los principios que deben dirigir su gestión por parte de empresas y organizaciones, como la transparencia o la exactitud de los datos. El RGPD ha establecido un marco de referencia en cuanto a la protección de datos.

Haz clic en el icono para acceder a más información sobre el RGPD

Para mayor comodidad, hemos resumido algunas de sus directrices más relevantes:

- **Consentimiento explícito**: A menos que haya una justificación legal, las entidades deben pedirnos permiso claro e informado para recopilar y procesar nuestros datos personales. Es fundamental que nos informen sobre qué datos recopilan y con qué fin.

[3] Reglamento (UE) 2016/679 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.

El proyecto APP-PI es una iniciativa realizada 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)

Facebook recopiló datos biométricos mediante reconocimiento facial sin pedir consentimiento explícito. Después de recibir quejas, eliminó estas plantillas faciales en 2021.

- **Portabilidad de los datos:** Tenemos derecho a recibir nuestros datos personales en un formato que sea fácilmente transferible a otra empresa o plataforma. Esto facilita la competencia y nuestra libertad para elegir proveedores de servicios.

Si nos cambiamos de operador de telefonía, tenemos derecho a que nuestros datos sean cedidos al nuevo operador que elijamos sin necesidad de hacer ningún trámite.

- **Minimalidad de los datos:** Solo se deben recoger y almacenar los datos estrictamente necesarios para ofrecer el servicio para el que se solicitan.

Si necesitan los datos de una persona para acceder a un espectáculo, no deberían solicitar información innecesaria como el DNI. Sin embargo, para viajar, es necesario proporcionar esa información porque el registro de viajeros es una obligación legal.

- **Derechos ARCO (Acceso, Rectificación, Cancelación, Oposición).**
    - **Derecho de Acceso:** Como usuarios, tenemos derecho a saber qué datos personales están almacenando las entidades y cómo los están utilizando.

El proyecto APP-PI es una iniciativa realizada 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)

Podemos preguntar al Delegado de Protección de Datos de cualquier empresa qué datos están guardando sobre nosotros.

- **Derecho de Rectificación:** Podemos solicitar la corrección de datos incorrectos o desactualizados, algo esencial para mantener la precisión y veracidad de la información.

Si un medio de comunicación o cualquier plataforma publica información falsa sobre nosotros, tenemos derecho a que se rectifique.

- **Derecho de cancelación**: Podemos pedir la eliminación de nuestros datos personales cuando ya no sean necesarios para los fines con los que fueron recogidos, o si retiramos nuestro consentimiento.

Al cambiar de operador de telefonía, tenemos derecho a que eliminen nuestros datos.

- **Derecho de oposición:** Podemos oponernos al tratamiento de nuestros datos personales en situaciones específicas, como cuando el procesamiento no está justificado o creemos que afecta negativamente a nuestros derechos.

Como vemos, el RGPD nos protege en diversos aspectos donde nuestra privacidad

Si una empresa utiliza nuestros datos para fines de marketing directo, podemos oponernos a este tratamiento.

El proyecto APP-PI es una iniciativa realizada 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)

podría verse comprometida. Sin embargo, **¿cuáles son las consecuencias para las entidades que incumplen esta normativa?**

El RGPD establece **sanciones significativas** para las empresas que incumplan la normativa, lo que ha incentivado a las organizaciones a desarrollar prácticas de gestión de datos más responsables. Para ayudar a las organizaciones a cumplir con su normativa, el RGPD previó la figura del **Delegado de Protección de Datos (DPD)**, cuya función es asesorar para garantizar el cumplimiento de la normativa.

3.2. Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

En España, la **Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)**[4], promulgada en diciembre de 2018, adapta el RGPD al marco legislativo español.

Haz clic en el icono para acceder a más información sobre esta ley

Además de seguir los principios del marco normativo de la UE, introduce una serie de derechos adicionales específicos para el contexto digital en nuestro país. Entre sus **puntos clave** se encuentran:

- **Derechos digitales en el ámbito laboral**: La normativa incluye medidas para proteger nuestros derechos en el ámbito laboral, como el derecho a la desconexión digital para los trabajadores, lo que ayuda a evitar la sobrecarga laboral y protege nuestra vida privada.

Nuestro empleador no puede obligarnos a responder mensajes fuera del horario laboral.

[4] Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y Garantía de los Derechos Digitales.

El proyecto APP-PI es una iniciativa realizada 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)

- **Derecho al olvido**: Este derecho nos permite solicitar la eliminación de datos personales que facilitamos para utilizar servicios digitales.

> Podemos pedir a una red social que elimine la información que tiene almacenada sobre nosotros.

- **Protección de los menores en el entorno digital**: La LOPDGDD establece medidas específicas para proteger los datos de menores, asegurando que su interacción con aplicaciones, redes sociales y servicios digitales esté regulada y supervisada, garantizando su privacidad en la red.

> Un centro educativo necesita el permiso explícito de los tutores legales antes de fotografiar al alumnado.

4. Conclusión

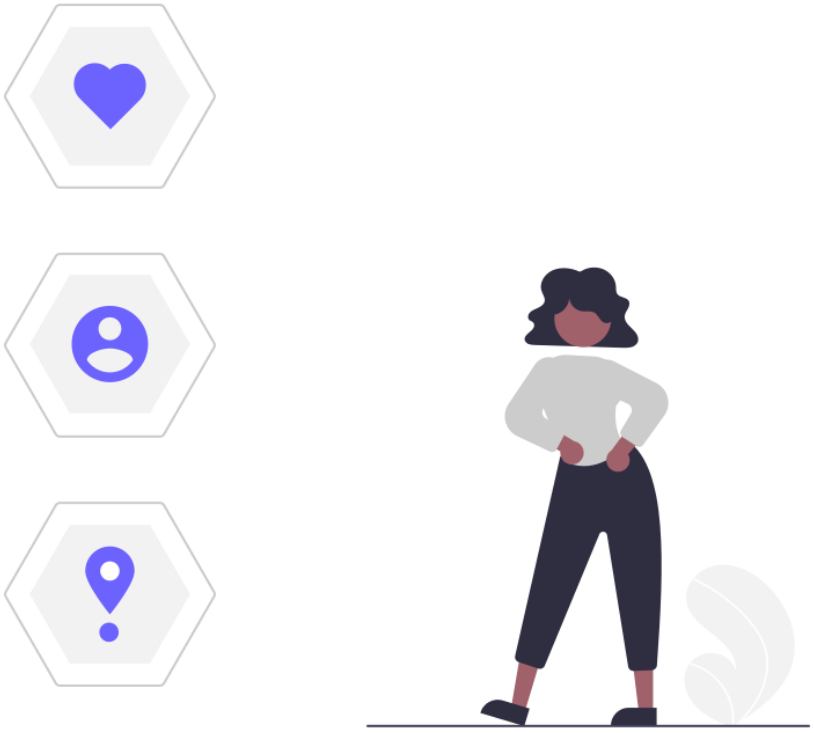
En resumen, la privacidad es un derecho esencial que ha evolucionado para enfrentar los desafíos del mundo digital. Proteger nuestra información personal es clave para garantizar nuestra seguridad, libertad y autonomía en un entorno cada vez más conectado. Normativas como el RGPD y la LOPDGDD han sido creadas para ayudarnos a mantener el control sobre nuestros datos, reforzando estos derechos en el ámbito digital.

Para entender mejor la privacidad, es importante reconocer cómo se relacionan los datos personales con ella y cómo desde la normativa que la regula se busca reducir los riesgos asociados a su recolección y uso. En el próximo módulo, profundizaremos en el concepto de datos personales, analizaremos quiénes están interesados en acceder a ellos y exploraremos los riesgos que enfrentamos si perdemos el control sobre nuestra información.

El proyecto APP-PI es una iniciativa realizada 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)

MÓDULO 2:

LOS DATOS PERSONALES



Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[5]

Universidad de Valladolid

gi.ingpriv@uva.es

[5]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz y Génesis M. De León Alcántara.

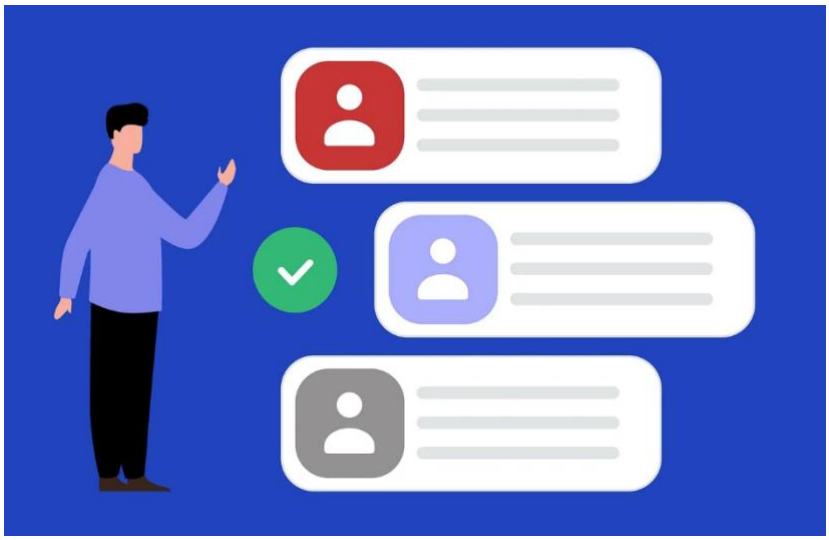
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Introducción

En la Sociedad de los Datos, con tantos dispositivos digitales a nuestro alrededor, nuestra privacidad depende de cómo protegemos nuestros datos personales. Como usuarios, es importante que entendamos qué son estos datos, quiénes pueden querer acceder a ellos y qué riesgos corremos si perdemos su control.

1. ¿Qué entendemos por datos personales?

Los datos personales son cualquier **información que permita identificar a una persona física**. Esto puede hacerse de manera **directa**, como con el DNI, o **indirecta**, combinando datos como la zona geográfica, la edad, el sexo o los hábitos de consumo, que por separado no identificarían a alguien, pero juntos podrían hacerlo.



Según la Comisión Europea, la protección de los datos personales es un derecho fundamental de todo ciudadano y las organizaciones que manejan este tipo de información deben aplicar esta protección con la máxima transparencia y respeto hacia los usuarios.

Algunos de los ejemplos más importantes de datos personales son los siguientes:

- **Nombre completo**: Nombre y apellidos.
- **Dirección física**: Nuestra ubicación geográfica, dirección de residencia, lugar de trabajo o lugares que frecuentamos.

El proyecto APP-PI es una iniciativa realizada 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)

- **Número de identificación**: Puede ser un número de Documento Nacional de Identidad, número de seguridad social o cualquier otra forma de identificación de un organismo o de un país.

- **Dirección de correo electrónico:** En este caso, el formato específico de un correo electrónico, como nombre.apellido@empresa.com, puede revelar tanto nuestra identidad como nuestro empleo.

- **Datos financieros**: Números de cuentas bancarias, tarjetas de crédito, transacciones financieras, entre otros.

- **Identificador de una cookie:** Las cookies son pequeños archivos que se almacenan en nuestro navegador cuando visitamos un sitio web y que pueden rastrear nuestro comportamiento en línea, como las páginas visitadas y las preferencias de búsqueda, lo que permite crear perfiles de usuario para publicidad y análisis.

- **Dirección IP o MAC**[6]: Identificador único de nuestro dispositivo cuando nos conectamos a internet. A través de la IP, se puede rastrear nuestra actividad en línea y nuestra ubicación aproximada. Conociendo la MAC se puede saber exactamente cuál es nuestro dispositivo.

- **Datos biométricos**: Incluye características físicas como huellas dactilares, reconocimiento facial o de voz.

No obstante, debemos saber que no todos los datos son personales, por ejemplo, los de empresas y los datos anonimizados:

- **Número de registro mercantil:** Identificador único de una empresa en el Registro Mercantil, utilizado para verificar su existencia y legalidad.

- **Dirección de correo electrónico:** Correo electrónico general de una empresa, como info@empresa.com, utilizado para la comunicación institucional.

[6] Media Access Control

El proyecto APP-PI es una iniciativa realizada 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)

- **Datos anonimizados:** Información procesada para eliminar la identificación personal, útil para análisis estadísticos sin comprometer la privacidad individual[7].

Haz clic en el icono para acceder a información sobre los datos personales proporcionada por la Comisión Europea:

2. ¿Quién puede querer acceder a nuestros datos?

En el entorno digital los datos personales son un recurso valioso que atrae a diversos actores con intereses distintos, que pueden ser desde ciberdelincuentes, que buscan apropiarse de ellos con fines maliciosos, hasta empresas legítimas y gobiernos, que recopilan, analizan y utilizan nuestros datos para diversos fines.

Los **principales actores** que podrían intentar acceder a nuestros datos personales:

1. **Ciberdelincuentes.**

Los ciberdelincuentes buscan explotar vulnerabilidades en dispositivos y aplicaciones para robar nuestros datos personales con fines maliciosos, que incluyen desde el robo de identidad y fraude financiero, hasta la venta de información personal.

Los ataques perpetrados por este tipo de agentes pueden adoptar diferentes formas, siendo común el uso de malware o “phising” para atacarnos de forma individual, o el uso de ataques directos a los servidores que almacenan datos personales.

[7] Según el Reglamento General de Protección de Datos (RGPD) los datos personales que se han anonimizado quedan fuera de su alcance.

El proyecto APP-PI es una iniciativa realizada 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 **malware**[8] es un software diseñado para infiltrarse en nuestros dispositivos y causar daño o robar datos.
- Un ejemplo de **"phising"** se daría en los correos electrónicos de remitentes que se hacen pasar por otras entidades y que contienen enlaces que, al abrirlos, descargan malware en nuestro dispositivo.
- Recientemente, el Banco Santander sufrió un **ciberataque** que dejó expuestos los datos personales de miles de sus clientes.

Haz clic en el icono para acceder a la noticia

Para estos delincuentes, los datos financieros como los números de tarjetas de crédito son particularmente valiosos, pero también lo son los correos electrónicos, direcciones y contraseñas.

2. **Empresas tecnológicas y de publicidad.**

Las empresas tecnológicas, de aplicaciones móviles y de redes sociales son los actores principales en la recopilación de datos personales a gran escala debido a que han convertido nuestros datos en una de sus principales fuentes de ingresos. Sus modelos de negocio suelen basarse en la recopilación y análisis de información personal para crear perfiles detallados de los usuarios que se utilizan para ofrecer a los anunciantes la posibilidad de pagar por publicidad altamente personalizada.

En resumen, las empresas tecnológicas se apropian de datos como nuestra ubicación, historial de búsquedas, interacciones en redes sociales y hábitos de compra para vender espacios publicitarios específicos a los anunciantes, quienes nos muestran anuncios personalizados según nuestra actividad online.

8

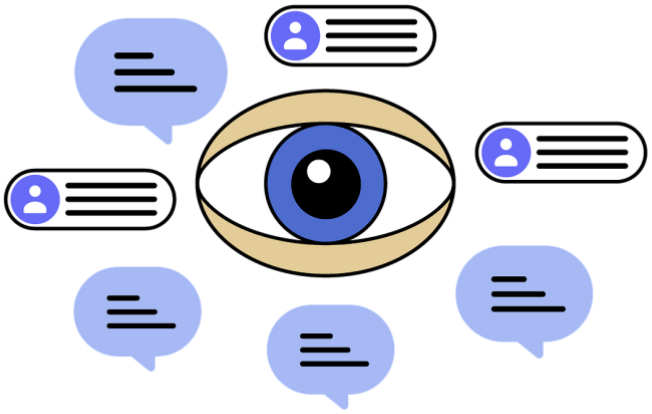
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Un ejemplo claro de esto son redes sociales como Instagram o TikTok, que están diseñadas para enganchar a los usuarios y hacer que pasen más tiempo en la plataforma, generando más datos sobre sus intereses y exponiéndose a un flujo mayor de publicidad.

Igualmente, los anunciantes y agencias de marketing también están interesados en obtener datos detallados sobre los consumidores para dirigir campañas publicitarias más efectivas. A menudo acceden a estos datos mediante acuerdos legales con plataformas tecnológicas.

3. **Gobiernos.**

Los gobiernos pueden solicitar o intentar acceder a nuestros datos personales con **fines de seguridad nacional** o **investigación criminal**, ya sea a través de **solicitudes legales** a empresas tecnológicas para acceder a datos de sus usuarios o mediante la implementación de medidas de vigilancia.



El hecho de que alguna normativa permita a las agencias de gobierno acceder a información personal **sin necesidad de una autorización judicial** genera preocupaciones sobre nuestra privacidad. Además, ya ha quedado demostrado que ciertos países tienen sistemas de vigilancia masiva que buscan monitorear actividades sospechosas.

¿Sabías qué...?

Uno de los escándalos más famosos es el causado por las revelaciones de Edward Snowden en 2013. Snowden, un excontratista de la Agencia de Seguridad Nacional de los Estados Unidos (NSA), reveló la existencia de un vasto programa de espionaje global llevado a cabo por el gobierno estadounidense. Sus filtraciones mostraron que la NSA y otras agencias recopilaban en secreto inmensas cantidades de datos de usuarios sin su conocimiento, incluidos registros telefónicos, correos electrónicos, historiales de navegación y mensajes en redes sociales.

Las filtraciones revelaron que este tipo de vigilancia no se limitaba solo a ciudadanos sospechosos de actividades delictivas, sino que afectaba a millones de personas en todo el mundo, incluyendo a países aliados, independientemente de que existiera o no una amenaza de seguridad. En concreto, en el caso de España se intervinieron 60 millones de llamadas telefónicas.

Este caso demostró que los gobiernos tienen la capacidad y la voluntad de acceder a enormes volúmenes de datos personales bajo el pretexto de seguridad nacional, lo que ha generado un debate global sobre los límites entre privacidad y seguridad y que ha llevado a preguntarse por la existencia de programas de este tipo en otros países.

El proyecto APP-PI es una iniciativa realizada 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)

4. **Compañías de análisis de datos.**

Las compañías de análisis de datos recopilan grandes cantidades de información para realizar estudios y análisis sobre nuestros patrones de comportamiento. Estos datos se utilizan para predecir tendencias, desarrollar productos y servicios o incluso influir en decisiones políticas. A menudo, estas empresas obtienen datos de terceros, lo que puede hacer que perdamos el control sobre la forma en que nuestra información es procesada.

¿Sabías qué...?

El ejemplo por excelencia de esta práctica es Cambridge Analytica, una empresa de análisis de datos que recopiló información personal de millones de usuarios de Facebook sin su consentimiento explícito. Posteriormente, dichos datos fueron usados para crear perfiles psicológicos detallados, permitiendo la creación de anuncios políticos personalizados durante las elecciones presidenciales de 2016 en los Estados Unidos y el referéndum del Brexit en el Reino Unido.

Esta empresa no solo recopiló datos directamente de los usuarios, sino que también obtuvo información de terceros a través de aplicaciones de Facebook, lo que permitió acceder a datos de personas que ni siquiera habían interactuado directamente con la empresa. Este caso reveló cómo las compañías de análisis de datos pueden influir en decisiones políticas y sociales mediante el uso de información personal, sin que los usuarios tengamos control total sobre cómo se procesan o utilizan nuestros datos.

El proyecto APP-PI es una iniciativa realizada 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)

5. **Desarrolladores de aplicaciones.**

Los desarrolladores de aplicaciones móviles suelen solicitar permisos para acceder a varios aspectos del dispositivo, como contactos, ubicación y cámara. Si bien muchas aplicaciones requieren estos datos para funcionar correctamente, algunas pueden abusar de los permisos solicitados para recopilar información personal sin que el usuario sea completamente consciente, lo que ocurre especialmente con aplicaciones gratuitas que basan su modelo de negocio en la recolección y venta de datos de los usuarios.

6. **Empleadores, bancos, compañías de seguros o instituciones educativas.**

En entornos laborales o educativos, los empleadores y las instituciones pueden tener acceso a ciertos datos personales de sus empleados o estudiantes, como el historial de navegación en dispositivos corporativos o institucionales. Aunque este acceso suele estar regulado, hay riesgos de que se utilice de manera indebida si no se protegen adecuadamente nuestros datos y nuestra privacidad.

El proyecto APP-PI es una iniciativa realizada 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)

3. ¿Qué puede ocurrir si perdemos nuestros datos?

Si perdemos nuestros datos personales, nos enfrentamos a consecuencias graves que afectan mucho más que nuestra privacidad. Nuestros datos pueden ser usados sin nuestro consentimiento para la **creación de perfiles comerciales**, lo que nos expone a

> MyHeritage, una empresa especializada en crear árboles genealógicos, analiza nuestro ADN y vende esos datos a las empresas de seguros, que pueden cobrarnos más si el análisis demuestra que somos propensos a padecer ciertas enfermedades.

recibir publicidad invasiva y dirigida basada en nuestros hábitos de consumo o navegación y nos deja vulnerables ante empresas que manejan nuestra información con fines lucrativos, a menudo sin que tengamos pleno control o conocimiento de cómo se están utilizando.

Además, **el robo o la suplantación de la identidad** se convierte en un riesgo inmediato si nuestros datos caen en manos equivocadas. Los ciberdelincuentes pueden utilizar nuestra información para **acceder a nuestras cuentas bancarias**, realizar compras no autorizadas o cometer fraudes a nuestro nombre.

Por otro lado, nuestra **libertad y seguridad** también se ven comprometidas si gobiernos u otros actores acceden a nuestros datos para **monitorear nuestras actividades**. La pérdida de control sobre nuestra información nos convierte en objetivos de vigilancia, afectando nuestra capacidad de mantener un entorno seguro y privado tanto en nuestra vida personal como profesional.

4. Conclusión

La protección de nuestros datos personales es clave en la era digital, ya que es fundamental para defender nuestra privacidad, seguridad y autonomía. La recolección y uso de datos por parte de diversos actores, como empresas tecnológicas, gobiernos y ciberdelincuentes, nos presenta grandes retos y riesgos. Si perdemos el control sobre nuestros datos, nuestra información personal puede quedar expuesta, poniendo en

El proyecto APP-PI es una iniciativa realizada 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)

peligro nuestros derechos, nuestra identidad, nuestra seguridad financiera, etc. Por eso, es importante que estemos al tanto de las amenazas y las herramientas disponibles para proteger nuestra privacidad. En los próximos módulos, profundizaremos en los factores principales que pueden comprometer nuestra seguridad en el entorno digital.

El proyecto APP-PI es una iniciativa realizada 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)

MÓDULO 3.

MALWARE

Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[9]

Universidad de Valladolid

gi.ingpriv@uva.es

[9]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz y Génesis M. De León Alcántara.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

En el módulo anterior hemos comentado qué son nuestros datos personales, cuáles son los peligros a los que nos enfrentamos si perdemos el control sobre estos y quiénes son los principales actores que están interesados en acceder a nuestros datos.

Hemos destacado el peligro procedente de los ciberdelincuentes, quienes pueden acceder a nuestros datos si los difundimos sin protegerlos en redes sociales y otras redes. También pueden hacerlo a través de ataques a los servidores que almacenan datos de forma masiva, o mediante malware.

En este módulo nos centramos en ese último aspecto, explorando en qué consiste el *malware*, cuáles son sus peligros y cómo podemos protegernos.

1. ¿Qué es el malware?

El **malware**, o **software malicioso**, son los programas diseñados para infiltrarse y dañar dispositivos y sistemas informáticos; es decir, programas que han sido creados con una intención delictiva.

Este tipo de software no solo puede dañar nuestros dispositivos, sino que también puede robar nuestros datos, causando un perjuicio a nuestra privacidad. En teléfonos, tabletas y ordenadores, el malware puede aprovechar los permisos que hemos otorgado a las aplicaciones para acceder a nuestra información personal.

El proyecto APP-PI es una iniciativa realizada 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)

Una forma en que el malware puede aprovecharse de nuestro comportamiento es infiltrándose en versiones pirateadas de apps de pago.

A medida que la tecnología avanza, el malware se está volviendo cada vez más sofisticado, lo que lo convierte en una de las principales amenazas en el ámbito digital. Su capacidad para adoptar diferentes formas y estrategias lo hace aún más peligroso; puede diseñarse para ser sigiloso, aprovechándose de vulnerabilidades del sistema o de las acciones (comportamiento) de las personas para infiltrarse en los dispositivos. El malware está en constante evolución, así que es esencial que estemos al tanto de las últimas tendencias y tipos de malware que circulan en la web.

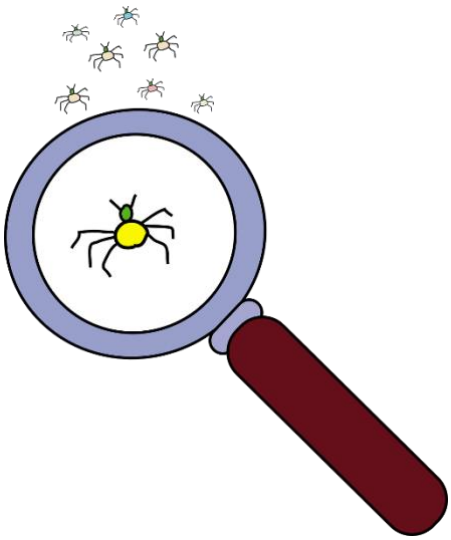
2. Tipos de malware

La historia del malware se remonta a los inicios de la informática. Uno de los primeros ejemplos de malware se encuentra en el Creeper, un programa autorreplicante que se creó en la década de 1970. Este programa no tenía intenciones maliciosas y se creó de forma experimental; su única función era desplegar en la pantalla del ordenador infectado el texto “I’m the creeper. Catch me if you can!”.

Con el auge de internet en las últimas décadas del siglo XX, el malware comenzó a evolucionar, enfocándose cada vez más en realizar actividades malintencionadas. A

El proyecto APP-PI es una iniciativa realizada 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)

medida que avanzaba, se diversificó en distintos tipos según el daño que puede causar y las estrategias que utiliza para infiltrarse en los equipos.



Actualmente existen muchos tipos de software malicioso. Aquí comentamos aquellos que afectan con más frecuencia a nuestra privacidad, destacando sus características y ofreciendo ejemplos de su uso.

7. **Virus:** Los virus se propagan al adherirse a otros programas o archivos, por lo que requieren que el usuario ejecute un archivo infectado para propagarse. Pueden dañar aplicaciones y archivos del sistema, ralentizando el dispositivo y robando información personal en el proceso.

> Podemos infectarnos con un virus al piratear un programa, como la versión gratis de aplicaciones como Spotify.

8. **Troyanos:** Los troyanos se hacen pasar por aplicaciones legítimas, engañándonos para que los instalemos. Una vez infiltrados, permiten que los atacantes accedan a datos sensibles, contraseñas o incluso a nuestra actividad en el dispositivo.

El proyecto APP-PI es una iniciativa realizada 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)

Los ciberdelincuentes pueden utilizar un troyano disfrazado de aplicación financiera para acceder a nuestros datos bancarios.

9. **Spyware:** El spyware recopila información sin nuestro conocimiento. Monitoriza actividades, pulsaciones de teclas y ubicación, enviando estos datos a terceros sin nuestro consentimiento.

Una de las aplicaciones de este malware sería el robo de claves bancarias, pudiendo registrar qué teclas pulsamos al ingresar una contraseña.

- **Ransomware:** Este tipo de malware "secuestra" nuestro dispositivo. Para ello bloquea el acceso a los archivos o a todo el dispositivo, exigiendo un pago para liberarlo.

Este software suele afectar más a organizaciones, siendo famosos los casos de WannaCry o CryptoLocker, que causaron pérdidas millonarias.

Haz clic en el icono para acceder a la noticia

El proyecto APP-PI es una iniciativa realizada 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)

3. Peligros del malware

Los peligros del malware son diversos y pueden tener consecuencias graves para nuestros dispositivos y nuestra información personal.

Para nosotros, como usuarios, el malware impacta en nuestra privacidad de las siguientes formas:

- **Robo de datos:** La forma más obvia en la que estos programas afectan nuestra privacidad es a través del robo de datos. Todos los tipos de malware presentados pueden utilizarse para acceder a información sensible, como contraseñas, información bancaria y datos de identificación personal, que puede ser utilizada de forma fraudulenta, para la suplantación de identidad o para el acceso no autorizado a diferentes cuentas.

- **Pérdida de datos:** En el caso de una infección con ransomware, que cifra nuestros datos y bloquea su acceso hasta el pago de un rescate, no solo

podemos estar perdiendo el control de nuestros datos, sino que podemos llegar a perder el acceso a ellos por completo.

A menudo las víctimas no recuperan su información incluso después de pagar. Si sufrimos un ataque de ransomware (o de cualquier otro tipo) debemos acudir a un profesional.

- **Invasión directa de la privacidad:** El spyware y otras formas de malware pueden espiar nuestras actividades, recopilando datos sobre nuestras preferencias y comportamientos.

Los efectos del malware sobre nuestra privacidad y seguridad son profundos y alarmantes. Para protegernos de forma eficaz, debemos entender **cómo se introduce el malware en nuestros dispositivos.**

El proyecto APP-PI es una iniciativa realizada 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)

4. ¿Cómo se introduce el malware en nuestros dispositivos?

Existen **numerosas vías** que los ciberdelincuentes explotan para conseguir su objetivo. Las más comunes son:

- **Descarga de aplicaciones de fuentes no confiables:** Descargar aplicaciones fuera de las tiendas oficiales, como Google Play Store o Apple App Store, es una vía común de infección. En las appstores no oficiales las aplicaciones que contienen no pasan por las revisiones de seguridad que realizan las plataformas oficiales. Esto hace que sea más fácil para los ciberdelincuentes infiltrar malware.

Google y Apple están incrementando el esfuerzo de eliminar malware, pero esto no significa que el riesgo de infección al descargar de tiendas oficiales sea nulo. La gran cantidad de aplicaciones que contienen hace que sea imposible filtrar todas ellas, por lo que existe la posibilidad de encontrar software malicioso en repositorios oficiales.

- **Redes sociales y correos electrónicos:** Es frecuente que el malware se distribuya a través de enlaces maliciosos en redes sociales o correos electrónicos. Los estafadores pueden utilizar tácticas de ingeniería social para engañarnos y hacer que cliquemos en enlaces que instalan malware en nuestros dispositivos.

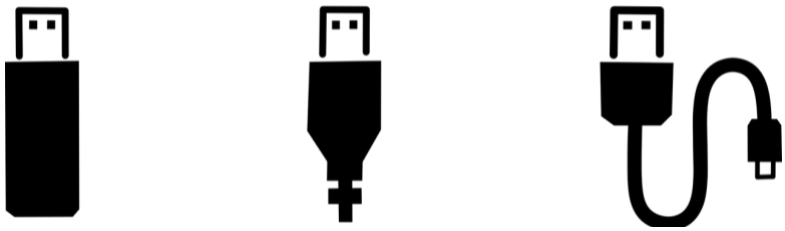
Es común que recibamos correos o mensajes de Whatsapp haciéndose pasar por nuestros bancos. En los últimos años las empresas suelen advertirnos de que no solicitan datos personales a través de enlaces.

El proyecto APP-PI es una iniciativa realizada 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)

- **Anuncios maliciosos:** De forma similar al punto anterior, algunos enlaces en línea suelen estar diseñados para redirigirnos a sitios web maliciosos o para descargar software no deseado automáticamente. Esta práctica se conoce como **malvertising** y es una técnica utilizada por ciberdelincuentes para propagar malware.

A todos se nos vienen a la cabeza anuncios curiosos que aparecen en páginas web. Hacer clic en ellos puede poner en peligro nuestros datos y dispositivos.

- **Dispositivos USB infectados:** El malware también puede introducirse a través de dispositivos USB o conectores USB infectados; si conectamos un USB que contiene malware a nuestro dispositivo podemos infectarlo si no tenemos la protección adecuada.



Nunca debemos introducir un USB en nuestros dispositivos si no proviene de una fuente de confianza.

5. **Redes Wi-Fi gratuitas**: Las redes Wi-Fi públicas y gratuitas pueden ser un punto de acceso para los ciberdelincuentes. Al conectarnos a una red Wi-Fi no segura, nos exponemos a que terceros accedan a nuestros datos, intercepten la

El proyecto APP-PI es una iniciativa realizada 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)

información que enviamos o recibimos, o instalen malware en nuestro dispositivo.

Si es necesario usar una red Wi-Fi pública, debemos asegurarnos de utilizar una VPN (Red Privada Virtual) para proteger nuestra conexión y evitar que nuestros datos sean accesibles a través de la red.

El malware puede llegarnos de muchas formas, desde descargando aplicaciones de fuentes no confiables hasta engaños más complejos. No obstante, podemos protegernos de esta amenaza aplicando una serie de medidas sencillas.

5. Consejos para protegernos contra el malware

Las estrategias sencillas que podemos adoptar para protegernos del malware son las siguientes:

Instalar un antivirus confiable: Es la medida más directa. Los antivirus son programas que analizan tanto las apps que ya tenemos instaladas como las nuevas descargas. Nos ayudan a identificar comportamientos anómalos o archivos maliciosos antes de instalarlos.

La mayoría de los antivirus ofrecen análisis en tiempo real para proteger nuestros dispositivos mientras navegamos por la web o descargamos archivos.

Haz clic en el icono para encontrar ejemplos de antivirus para Android.

Revisar la fuente de descarga: Esta medida, igual de importante que la anterior, consiste en tratar de descargar las aplicaciones desde tiendas oficiales como Google Play Store o Apple App Store, que revisan las aplicaciones y reducen el riesgo de malware. Si descargamos desde un sitio web, debemos investigar su reputación y fiabilidad.

Un alto número de reseñas negativas o críticas sobre el comportamiento de la aplicación son banderas rojas; además, si algunas de ellas mencionan publicidad invasiva o acciones extrañas debemos evitar descargar esa app.

Verificar el desarrollador: El malware puede estar presente también en los repositorios oficiales. Es importante verificar el desarrollador de la aplicación que queremos descargar, asegurándonos de que es fiable a través de las reseñas de esa app y del resto de las creadas por esa entidad.

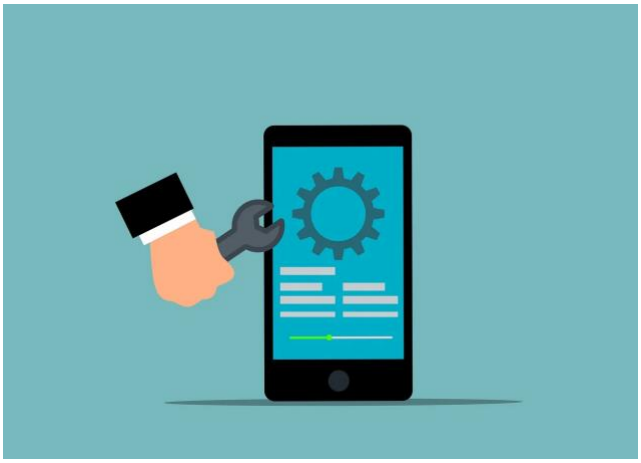
Evaluar los permisos solicitados: Las aplicaciones maliciosas suelen pedir más permisos de los necesarios. Debemos cuestionar la necesidad de esos permisos y considerar si la aplicación realmente requiere esos accesos para funcionar.

El proyecto APP-PI es una iniciativa realizada 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)

Si una app de linterna, por ejemplo, solicita acceso a nuestros contactos o nuestra ubicación, es una señal de alerta.

Evitar enlaces o descargas sospechosas: Debemos ser muy cautelosos con enlaces que recibimos a través de correos electrónicos, redes sociales o mensajes de texto, especialmente si provienen de fuentes desconocidas. Si desconfiamos de un email o un mensaje de Whatsapp no debemos abrirlo.

Mantener actualizado el sistema operativo y las aplicaciones: Los desarrolladores descubren con frecuencia vulnerabilidades que pueden ser explotadas en sus aplicaciones, que solucionan en forma de actualizaciones que no solo mejoran las funciones de la app, sino que también sirven como parches de seguridad.



No utilizar WIFIs gratuitas o sin contraseña: Las redes Wi-Fi abiertas o gratuitas no cuentan con medidas de seguridad suficientes para proteger nuestra información. Al conectarnos a estas redes, nuestros datos pueden ser interceptados fácilmente por ciberdelincuentes que se encuentren en la misma red. Si necesitamos utilizar una, debemos hacerlo utilizando una VPN.

Otros repositorios

Como pequeño apunte, también existen repositorios de software que son utilizados, sobre todo, en entornos de código abierto o por **usuarios más avanzados**. Un ejemplo de estos es F-Droid, un repositorio popular para dispositivos Android donde podemos encontrar aplicaciones libres y de código abierto. No obstante, **su uso se desaconseja**

Un ejemplo de market alternativo es Aptoide

Optar por repositorios alternativos puede hacernos más vulnerables ante ataques con malware.

Para minimizar el riesgo de infección y proteger nuestra privacidad, es fundamental descargar aplicaciones solo desde tiendas oficiales como Google Play Store y Apple App Store.

El proyecto APP-PI es una iniciativa realizada 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)

al resto de usuarios, pues el **riesgo de infección es mayor.**

Importante…

Incluso las aplicaciones que no contienen malware pueden afectar a nuestra privacidad y recopilar nuestros datos personales.

6. Conclusión

El malware supone una amenaza constante a nuestra privacidad que nos acecha mientras realizamos cualquiera de las tareas digitales habituales en nuestra vida diaria.

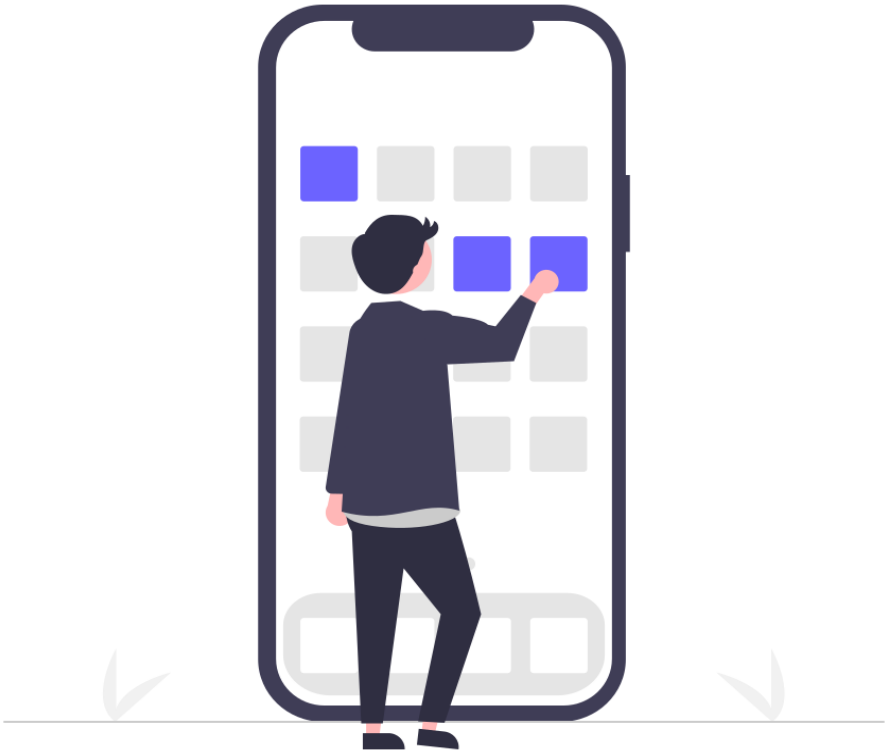
En este módulo hemos aprendido que este puede presentarse en diferentes formas, puede infectarnos de múltiples maneras y puede poner en peligro el control que tenemos sobre nuestros datos personales. Afortunadamente, existen varias medidas de fácil aplicación que podemos tomar para reducir el peligro de infección, incluyendo el uso de herramientas como antivirus. Por desgracia, en el mundo actual nuestros datos personales no solo interesan a los ciberdelincuentes, sino que existen numerosos actores que tratan de acceder a ellos de diferentes formas.

Como veremos en el **próximo módulo**, **los programas que amenazan a nuestra privacidad no se limitan al malware, siendo igualmente intrusivas muchas de las aplicaciones que utilizamos en nuestro día a día.**

El proyecto APP-PI es una iniciativa realizada 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)

MÓDULO 4.

APLICACIONES MÓVILES



Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[10]

Universidad de Valladolid

gi.ingpriv@uva.es

[10]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz y Génesis M. De León Alcántara.

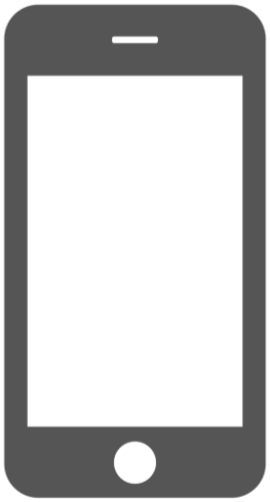
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Introducción

En la era digital, las aplicaciones móviles se han convertido en herramientas esenciales en nuestra vida cotidiana. Más allá de su utilidad, las aplicaciones móviles pueden representar riesgos significativos para nuestra privacidad, ya que la información que compartimos a través de ellas puede ser utilizada sin nuestro pleno conocimiento o consentimiento. **Incluso si una aplicación no es maliciosa**, puede recopilar una gran cantidad de datos que luego pueden ser utilizados con fines publicitarios, vendidos a terceros, o incluso vulnerados en caso de brechas de seguridad. En este módulo, analizaremos cómo acceden a nuestros datos y los peligros asociados a su manejo.

1. ¿Qué es una aplicación?

Una aplicación es un software diseñado para realizar tareas específicas en dispositivos como teléfonos móviles, ordenadores o tablets. Las aplicaciones facilitan actividades tan diversas como la comunicación, la gestión de finanzas, el entretenimiento o el aprendizaje, adaptándose a nuestras necesidades de forma eficiente y accesible.



Estas herramientas digitales pueden clasificarse según el dispositivo para el que están diseñadas; algunas están optimizadas para móviles y tablets, mientras que otras se desarrollan para ordenadores. En este módulo nos centramos en las apps, que están creadas para sistemas operativos como Android e iOS, ofreciendo una interfaz adaptada a pantallas más pequeñas y funciones específicas que simplifican su uso.

El proyecto APP-PI es una iniciativa realizada 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)

Muchas de ellas requieren acceso a recursos del dispositivo, como la cámara, el micrófono o el GPS, lo que permite experiencias avanzadas como la navegación en tiempo real, el escaneo de códigos QR o el uso de filtros graciosos en aplicaciones como Instagram o TikTok. Sin embargo, algunas también recopilan datos personales, por lo que es fundamental revisar los permisos que otorgamos y limitar la instalación a fuentes confiables.

2. Privacidad en riesgo: más allá del malware

En el módulo anterior ya hemos visto lo que es un malware pero no todas las amenazas a la privacidad provienen de virus o apps maliciosas. **Muchas aplicaciones legítimas y populares pueden ser altamente intrusivas sin ser técnicamente malware.** Esto ocurre cuando recopilan o comparten datos personales de formas que no están claramente informadas ni consentidas por el usuario.

Por ejemplo:

- **La app del BBVA**, fue señalada por compartir datos con terceros sin pedir un consentimiento explícito, lo que generó gran preocupación sobre la transparencia en el uso de la información financiera de los usuarios.
- Durante la pandemia, el gobierno español lanzó una app oficial para el rastreo de contactos COVID-19 que fue duramente cuestionada por **fallos graves de privacidad**, como la falta de claridad sobre el destino de los datos recopilados y el nivel de anonimato ofrecido.
- **WhatsApp**, uno de los servicios de mensajería más usados del mundo, el cual ha sido varias veces sancionado por la Unión Europea por vulnerar la normativa de protección de datos. Los problemas han incluido formas poco transparentes de recabar el consentimiento para compartir datos con otras empresas del grupo Meta, así como **la vulneración del derecho al olvido**, es decir, la dificultad o imposibilidad de eliminar completamente tus datos.

Estos ejemplos muestran que incluso apps ampliamente utilizadas pueden tener prácticas opacas en cuanto a privacidad. **No hace falta que una app contenga**

El proyecto APP-PI es una iniciativa realizada 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)

malware para ser un riesgo: basta con que recopile, procese o comparta tus datos sin la debida transparencia o sin darte la opción real de negarte.

3. ¿Dónde conseguimos las aplicaciones móviles?

Tiendas oficiales

Para descargar una aplicación móvil **es recomendable** recurrir a **tiendas oficiales** como Google Play Store para dispositivos Android o Apple App Store para dispositivos iOS.

Las tiendas oficiales como Google Play Store y Apple App Store son gestionadas por los fabricantes de los sistemas operativos, lo que garantiza ciertos controles de calidad y seguridad en las aplicaciones que ofrecen. Sin embargo, debido a la gran cantidad de aplicaciones disponibles, no todas pasan un filtrado completamente efectivo, por lo que podemos encontrar apps maliciosas incluso en estas plataformas.

Tiendas alternativas

Como usuarios podemos encontrar otras tiendas que pueden parecer muy atractivas.

Su uso es peligroso, pues las apps que contienen pueden haber sido alteradas por un tercero.

Al descargar aplicaciones de estas tiendas corremos un mayor riesgo de infectarnos con malware. Por ejemplo: al descargar la aplicación de nuestro banco desde un sitio alternativo es posible que terceros accedan a nuestros datos bancarios

El proyecto APP-PI es una iniciativa realizada 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)

4. Los permisos

Los **permisos** son la forma en la que las aplicaciones solicitan acceder a recursos o datos almacenados en nuestro dispositivo. Cuando una aplicación necesita utilizar un recurso de nuestro dispositivo, como la cámara, o el almacenamiento, debemos concederle el permiso para acceder a ese recurso. Los permisos son necesarios para que las aplicaciones funcionen correctamente (hagan aquello para lo que se han creado) o para mejorar la experiencia del usuario.

Sin embargo, **en muchos casos las apps solicitan acceso a recursos que no son necesarios para su operación principal.** Por tanto, si no conocemos los permisos que estamos otorgando nuestra privacidad y seguridad pueden verse comprometidas.

Por eso, gestionar los permisos adecuadamente es fundamental para minimizar el riesgo de exponer nuestros datos personales.

Una app con acceso a nuestra ubicación puede rastrear nuestros movimientos a lo largo del día y vender esa información a empresas que la utilicen para enviar publicidad geolocalizada.

El proyecto APP-PI es una iniciativa realizada 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)

Whatsapp pide acceso a los contactos del teléfono y Google Maps pide permiso para conocer nuestra ubicación, facilitando el establecimiento de rutas.

4.1. Tipos de permisos

En primer lugar, podemos dividir los permisos en dos tipos:

- **Permisos que NO podemos controlar:** Permisos que las aplicaciones solicitan **en el momento de la instalación**; son necesarios para que esta se lleve a cabo. Al decidir instalar una aplicación los estamos aceptando de forma automática.

Una aplicación puede requerir acceso a la cámara o a los contactos para funcionar correctamente. En algunos casos, si no aceptamos estos permisos, no podremos instalar la aplicación o la app no podrá funcionar como esperamos.

- **Permisos que SÍ podemos controlar:** Los permisos anteriores se aceptan durante el proceso de instalación de la aplicación. Los que se presentan ahora se solicitan y deben ser aceptados **después de la instalación**, durante la ejecución de la app. En este caso SÍ que tenemos un mayor control sobre qué recursos y funcionalidades del dispositivo pueden ser utilizados; en próximos módulos exploraremos cómo hacerlo.

¿Sabías qué...?

Aunque estos son los que tradicionalmente conocemos por el nombre de "permisos", realmente consisten en **grupos de permisos**, que engloban un gran número de permisos individuales. Por ejemplo, al revocar el permiso a acceder a los SMS en realidad estamos revocando un grupo de muchos permisos individuales relacionados con esa función.

El proyecto APP-PI es una iniciativa realizada 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)

Los permisos más comunes a los que suelen solicitar acceso las aplicaciones son:

1. **Acceso a la cámara:** Permite tomar fotos y vídeos.
2. **Acceso al micrófono:** Permite grabar audio.
3. **Acceso a los contactos:** Permite leer y modificar la lista de contactos del dispositivo.
4. **Acceso a la ubicación:** Utiliza el GPS para rastrear la posición del usuario.
5. **Acceso a archivos:** Permite leer, modificar o eliminar archivos del dispositivo.

A través del "Internet of Things" pueden filtrarse datos tan sensibles como fotos personales o un plano de nuestra vivienda. Un ejemplo sería el escándalo de iRoomba, marca de robots de limpieza que guardaba la localización de nuestra vivienda, la mapeaba y tomaba fotos de su interior. Esos datos terminaban filtrándose en la red.

¿Sabías qué...?

Haz clic en el icono para acceder a la noticia

4.2. ¿Cómo podemos saber qué permisos utilizan las aplicaciones?

Es importante que conozcamos qué datos recopilan las aplicaciones que utilizamos para proteger nuestra privacidad. Para ello, existen diversas formas de acceder a esta información, antes y después de la instalación de una aplicación.

Política de privacidad de la aplicación.

Las políticas de privacidad son **obligatorias** para las aplicaciones y deben detallar **de manera clara y comprensible** qué datos personales recopilan, cómo se utilizan, con qué fin, con quién se comparten y qué derechos tiene el usuario sobre su información.

El proyecto APP-PI es una iniciativa realizada 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)

Aunque la normativa establece que deben ser claras, **muchas veces no están redactadas en un lenguaje accesible**.

> Las políticas de privacidad de las grandes empresas tecnológicas, como Google, suelen ser extensas y complejas, lo que puede dificultar que comprendamos adecuadamente cómo se recopilan y utilizan los datos que proporcionamos cuando utilizamos sus servicios.

Es **importante leer las políticas de privacidad antes de aceptar los términos de uso**. Sin embargo, la realidad es que no solemos tomarnos el tiempo de revisar estos documentos.

1) Facilidad de acceso a las políticas de privacidad:
En general, acceder a ellas no es difícil. Podemos encontrar la política de privacidad en la configuración de la aplicación, en la tienda de apps antes de instalarla o a través de enlaces que aparecen durante la instalación o configuración inicial.

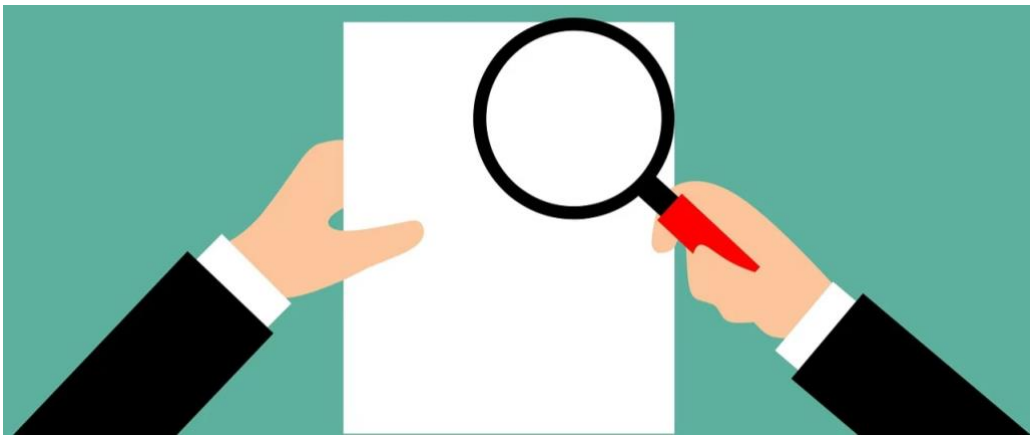
2) Problema de legibilidad:
Aunque el acceso sea sencillo, el contenido suele presentar obstáculos importantes: están redactadas con lenguaje legal complejo, excesivamente extenso o ambiguo, lo que dificulta su comprensión para la mayoría de las personas. Esto representa un problema clave en la toma de decisiones informadas sobre el uso de nuestros datos personales.

En ocasiones, las aplicaciones **también nos redirigen a su política de privacidad durante la instalación o configuración inicial.**

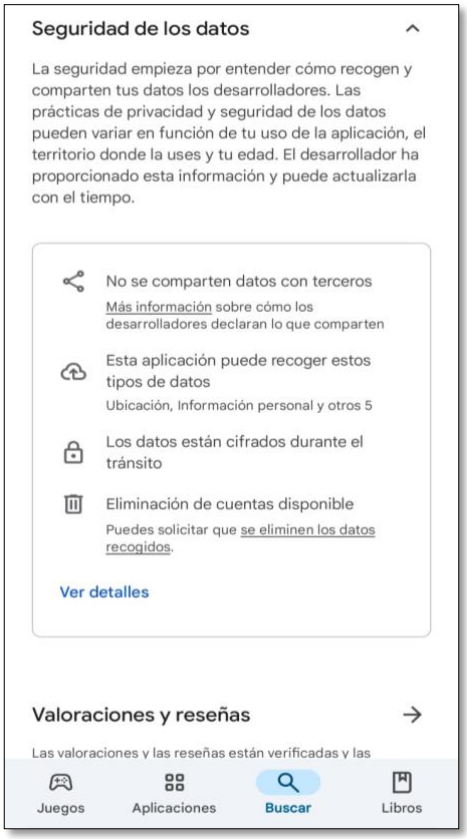
Descripción de permisos en las tiendas de aplicaciones.

Google Play ha incorporado la sección **"Seguridad de los datos"**, que aparece en la página de cada aplicación incluso antes de su instalación. Esta sección informa, de forma resumida, **qué datos puede recopilar una app, si se comparten con terceros, y cómo los protege**.

El proyecto APP-PI es una iniciativa realizada 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)



En esta imagen de ejemplo, se destacan cuatro puntos clave:



1. **No se comparten datos con terceros**: Esto significa que la app declara no enviar tu información a otras empresas, aunque esta afirmación depende de la honestidad del desarrollador.
2. **Tipos de datos que puede recoger**: Por ejemplo, ubicación, información personal, o actividad dentro de la app.
3. **Datos cifrados durante el tránsito**: Tus datos están protegidos mientras viajan entre tu dispositivo y los servidores de la app.
4. **Eliminación de cuentas disponible**: Puedes solicitar que se borren tus datos si dejas de usar el servicio.

Luego, al pulsar **"Ver detalles"**, se despliega información como la que muestra la **segunda imagen aquí debajo**, donde se especifican con más claridad los tipos de datos que podrían recopilarse. Por ejemplo:

- **Información personal**: como tu correo o número de teléfono.
- **Ubicación**: si se usa el GPS del teléfono.

El proyecto APP-PI es una iniciativa realizada 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)

- **Información financiera**: si haces pagos dentro de la app.
- **Actividad en la aplicación**: como búsquedas o interacciones que realizas.

¿Por qué es importante?

Este tipo de información nos permite tomar decisiones más informadas antes de instalar una aplicación. Aunque no todas las apps son peligrosas, algunas pueden recopilar más datos de los que realmente necesitan para funcionar. Entender esta sección te ayuda a proteger mejor tu privacidad.

Por lo tanto, es importante que adquiramos la costumbre de revisar la descripción de los permisos que solicita cada aplicación en las plataformas oficiales.

El proyecto APP-PI es una iniciativa realizada 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)

Solicitudes explícitas por parte de las apps.

Una vez que instalamos una aplicación, las solicitudes de permisos suelen aparecer durante la ejecución. Las apps nos pedirán acceso a ciertos datos o recursos del dispositivo antes de realizar alguna función específica. Por ejemplo:

- Acceso a la cámara: Si la aplicación necesita tomar fotos o vídeos, solicitará permiso para acceder a la cámara.
- Acceso a la ubicación: Si la app necesita saber tu ubicación, te pedirá permiso para acceder a la función GPS.

Otras fuentes externas.

También existen fuentes externas que analizan y detallan la privacidad de las aplicaciones. Estos servicios o páginas web suelen ofrecer revisiones detalladas sobre cómo maneja cada app los datos de sus usuarios y su nivel de transparencia en cuanto a la recopilación de información. En el siguiente módulo se dará más información sobre esas herramientas y su uso.

4.3. ¿Cómo podemos gestionar esos permisos?

Es fundamental cuestionarnos si una aplicación realmente necesita los permisos solicitados para cumplir con su función principal. Cada vez que una app solicita acceso a recursos sensibles como la cámara, micrófono, contactos, ubicación o archivos, estamos cediendo parte de nuestro control sobre estos datos.

Para ello, existen diversas herramientas que nos permiten tener un mayor control sobre los permisos de las aplicaciones, como **APK Falcon** o **Exodus Privacy**, que nos proporcionan información detallada sobre los permisos que las apps solicitan y cómo afectan a nuestra privacidad. Además, es importante saber que **podemos gestionar manualmente ciertos permisos una vez que las aplicaciones están instaladas en nuestro dispositivo.**

Exploraremos esto en detalle en los dos últimos módulos de este curso.

5. Conclusión

En este módulo hemos explorado cómo las aplicaciones móviles, aunque nos brindan comodidad y funcionalidad, pueden conllevar riesgos para nuestra privacidad, recopilando una cantidad considerable de datos personales. Así, hemos aprendido sobre los permisos. Aunque sirven para personalizar y mejorar la funcionalidad de las apps, pueden ser aprovechados de formas que no siempre son transparentes o seguras.

Por tanto, para proteger nuestros datos personales es fundamental que tomemos conciencia de los permisos que otorgamos a las aplicaciones y de cómo gestionarlos, tanto durante la instalación como durante el uso de las apps.

En futuros módulos exploraremos las diversas herramientas y recursos que pueden ayudarnos a comprender y gestionar los permisos. Veremos cómo activar o desactivar permisos de forma manual y cómo realizar pruebas antes de instalar a través de las plataformas APKFalcon y Exodus Privacy, que ofrecen información valiosa sobre los permisos solicitados por las apps y su impacto en nuestra privacidad.

El proyecto APP-PI es una iniciativa realizada 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)

MÓDULO 5.

TOMANDO EL CONTROL I

Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[11]

Universidad de Valladolid

gi.ingpriv@uva.es

[11]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

En el mundo actual, las aplicaciones móviles son herramientas esenciales que facilitan nuestras actividades diarias. Sin embargo, como hemos visto, muchas de ellas requieren permisos para acceder a recursos o datos sensibles de nuestros dispositivos, como la cámara, el micrófono o nuestra ubicación; desafortunadamente, aunque algunos permisos son necesarios para que las apps funcionen correctamente, otros pueden poner en riesgo nuestra privacidad si no los gestionamos con cuidado.

Por suerte, los dispositivos actuales nos ayudan a tener cierto control sobre nuestra privacidad, permitiéndonos gestionar ciertos grupos de permisos. En este módulo nos centraremos en una cuestión clave: cómo gestionar esos permisos en dispositivos Android.

A continuación, aprenderemos a identificar qué permisos han sido otorgados, cómo revocarlos o concederlos según nuestras necesidades, y exploraremos buenas prácticas que nos permitirán mantener un control más estricto sobre nuestra información.

El sistema operativo “Android” nos permite personalizar y ajustar los permisos de diferentes maneras.

El proyecto APP-PI es una iniciativa realizada 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)

1. Opciones para gestionar permisos en Android

Antes de comenzar la explicación, es importante resaltar que **lo que se explica en este módulo puede cambiar según la versión de Android**; aunque, de forma general, los pasos a seguir serán similares. Cuando hablamos de gestionar los permisos en Android, existen dos formas principales de hacerlo:

1. **Desde la configuración general:** entrando en la sección de "Permisos" a través de los Ajustes del dispositivo, podemos ver qué aplicaciones utilizan cada tipo de permiso.

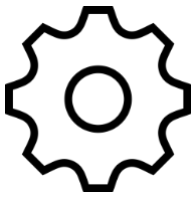
2. Seleccionando una aplicación específica: buscando la app cuyos permisos queremos comprobar en la sección "Aplicaciones" de los Ajustes. Una vez seleccionada, podemos ver los permisos utilizados por esa app en particular.

1.1 Gestión de permisos desde la configuración general

Esta opción es útil si queremos obtener una visión global de los permisos otorgados en nuestro dispositivo, pudiendo verificar, por ejemplo, todas las apps que tienen acceso a nuestra cámara o ubicación.

Pasos a seguir:

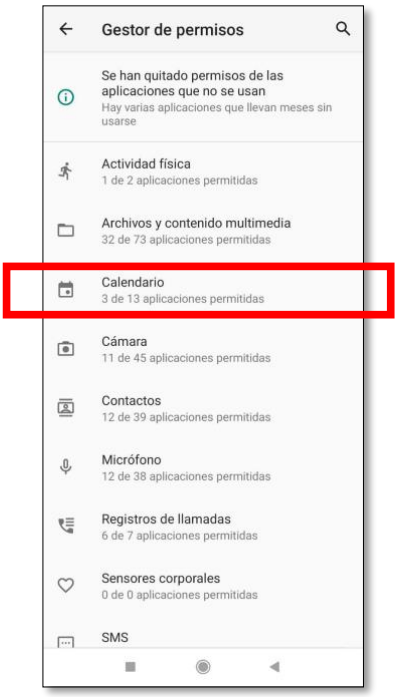
1. **Accedemos a la configuración del dispositivo:**
    - Para ello pulsamos en el icono de ajustes (con forma de engranaje) en el menú principal o en la bandeja de aplicaciones.



El proyecto APP-PI es una iniciativa realizada 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)

2. **Buscamos la sección de "Privacidad" o "Permisos de aplicaciones".**

   - Dependiendo de la versión de Android el nombre puede cambiar, pudiendo estar el gestor de permisos dentro de la sección de "Privacidad".
   - Dentro de la sección dedicada a la gestión de permisos podremos ver una pantalla similar a la siguiente.



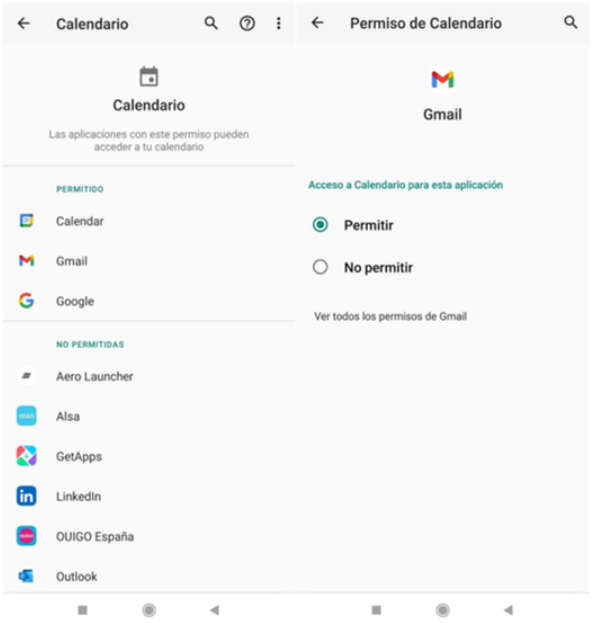
Como podemos observar en la imagen, desde aquí se pueden ver los permisos que se pueden gestionar y el número de aplicaciones que los utilizan. Para ver con más detalle qué app tiene concedido un permiso en particular, tenemos que pulsar encima del que nos interesa.

3. **Seleccionamos el tipo de permiso.**

Si seleccionamos un permiso, por ejemplo: "Calendario", podemos ver cada una de las apps a las que hemos concedido ese permiso, y a qué apps no lo hemos hecho. Es posible seleccionar las aplicaciones de forma individual para variar nuestra decisión para cada una de ellas.

El proyecto APP-PI es una iniciativa realizada 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)

En las imágenes siguientes se dan ejemplos de lo que se vería al seleccionar el de permiso “Calendario” y de lo que veríamos si eligiésemos gestionarlo para la aplicación “Gmail”.



Esta es una forma muy sencilla de obtener una imagen global del estado de los permisos en nuestro dispositivo. Sin embargo, en ocasiones necesitamos acceder a información específica sobre alguna aplicación en particular, en cuyo caso sería tedioso tener que analizar el estado de todos los permisos uno a uno. Por tanto, para comprobar qué permisos utiliza una app en particular es mucho más cómodo seguir el procedimiento que explicamos en el siguiente apartado.

1.2. Gestión de permisos desde la configuración de una aplicación específica

Este método es ideal si queremos ajustar los permisos de una app en a la que queremos retirar permisos. El proceso sería el siguiente:

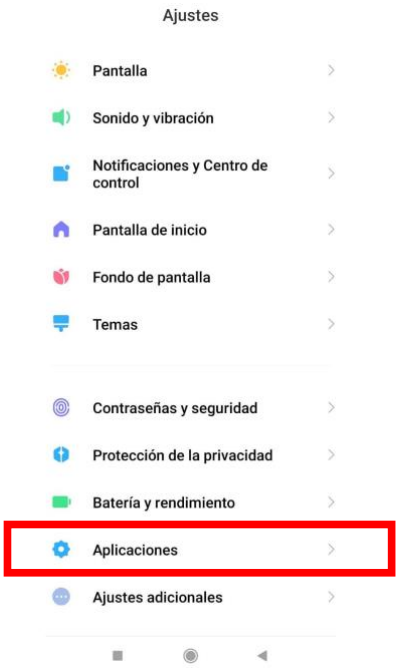
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Pasos a seguir:

1. Abrimos los ajustes del dispositivo.

Al igual que antes, accedemos al icono con forma de engranaje.

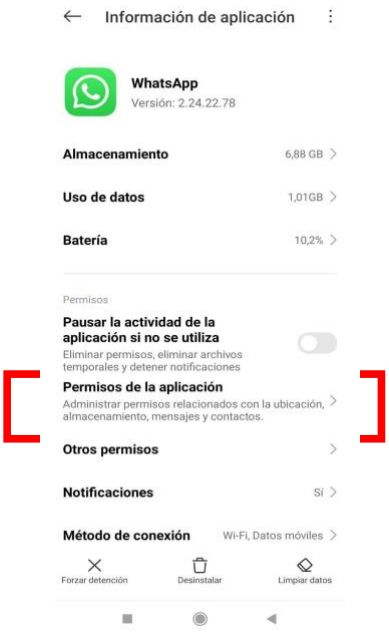
2. Buscamos la sección "Aplicaciones" o "Apps".



- Dependiendo de la versión de Android el nombre de esta sección puede variar, pudiendo llamarse “Apps”, “Aplicaciones”, “Aplicaciones y notificaciones”, etc.

3. Seleccionamos la app en cuestión.

- Dentro de la sección de “Aplicaciones”, puede que encontremos diferentes opciones, seleccionamos la que se llama “Administrador de aplicaciones”, donde encontraremos una lista con todas las que tenemos instaladas. Elegimos aquella cuyos permisos queremos gestionar. Para esta demostración vamos a seleccionar Whatsapp; una vez lo hayamos hecho, veremos una pantalla como la de la abajo a la derecha.



4. Acedemos a los permisos y los personalizamos.

- En la sección “Permisos de la aplicación”, podemos seleccionar aquellos que queremos conceder o denegar. La versión de Android que estamos utilizando nos proporciona además otras opciones para gestionar los permisos de esta app, dándonos la opción de revocarlos o concederlos.

El dominio de estos dos sencillos procedimientos nos otorga un control significativo sobre las aplicaciones que utilizamos.

El proyecto APP-PI es una iniciativa realizada 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)

2. Buenas prácticas en la gestión de permisos

Gestionar los permisos de forma eficiente no se limita a concederlos o denegarlos. También implica adoptar una serie de buenas prácticas que pueden elevar nuestro nivel de protección.

1. **Revisar los permisos periódicamente:** Las actualizaciones de las aplicaciones pueden modificar los permisos que hemos otorgado. Debemos dedicar un momento cada cierto tiempo para revisarlos y asegurarnos de que sigan siendo necesarios.

2. **Otorgar permisos solo cuando sean imprescindibles:** Si una app pide acceso a funciones o datos que no parecen estar relacionados con su propósito, tenemos que considerar no autorizarlos. Es importante que reflexionemos antes de aceptar, ya que muchos permisos no son esenciales para que una aplicación funcione correctamente.

3. **Utilizar permisos temporales siempre que sea posible:** En las versiones más recientes de Android, podemos conceder permisos "solo mientras se usa la app". Esta opción es ideal para limitar el acceso a nuestros datos cuando la aplicación no está activa.

4. **Desconfiar de apps desconocidas o de fuentes no oficiales:** Es recomendable que descarguemos aplicaciones únicamente desde Google Play Store u otras plataformas confiables. Las apps de fuentes no verificadas pueden comprometer nuestros datos.

5. **Mantener nuestro dispositivo actualizado:** Las nuevas versiones de Android suelen incorporar mejoras importantes en seguridad y gestión de permisos. Tener nuestro sistema operativo al día nos brinda más herramientas para proteger nuestra privacidad.

El proyecto APP-PI es una iniciativa realizada 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)

3. Conclusión

La gestión eficiente de los permisos en nuestros dispositivos móviles es fundamental para garantizar nuestra privacidad, proteger nuestra información personal. Sin embargo, a menudo puede ser difícil determinar cuáles son realmente necesarios y qué aplicaciones podrían estar recopilando datos de manera innecesaria.

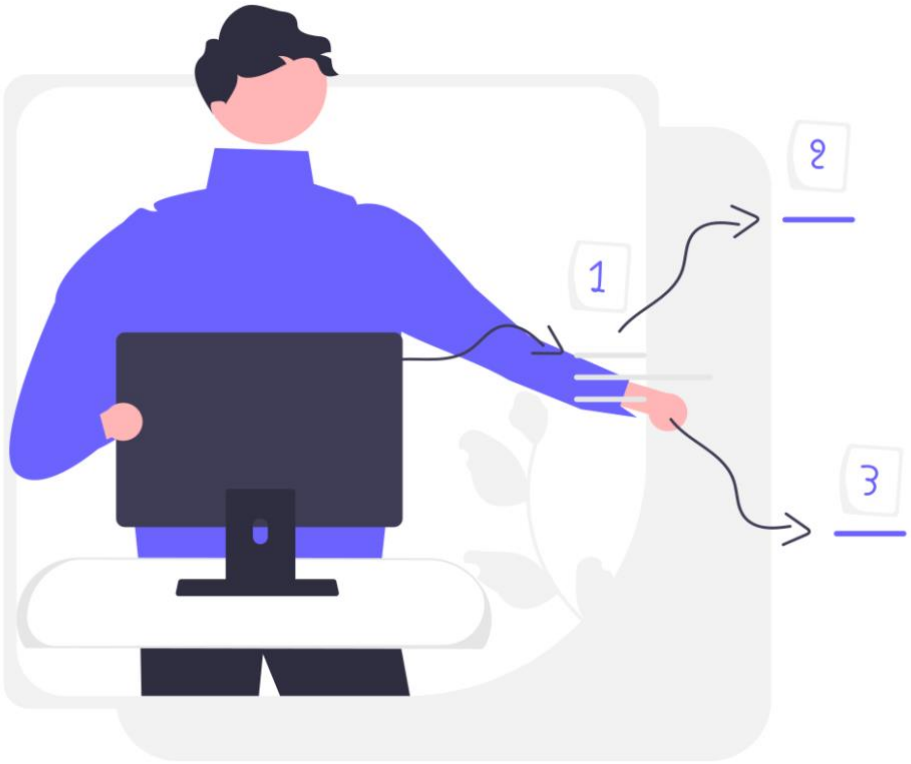
Además, solo podemos gestionar ciertos permisos, habiendo otros permisos que, como explicamos en el módulo 4, se aceptan automáticamente al instalar una aplicación y no podemos revocar una vez instalada.

Aquí es donde herramientas especializadas como *APKFalcon* o *Exodus Privacy* pueden marcar una gran diferencia, pues nos dan la posibilidad de hacer pruebas antes de instalar una aplicación, proporcionándonos una visión clara y detallada de los permisos que solicitan y los rastreadores que incluyen. En el siguiente y último módulo hablaremos sobre las características de esas plataformas y proporcionaremos instrucciones para su uso.

El proyecto APP-PI es una iniciativa realizada 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)

MÓDULO 6.

TOMANDO EL CONTROL II



Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[12]

Universidad de Valladolid

gi.ingpriv@uva.es

[12]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

En el módulo anterior hemos aprendido a gestionar los permisos de las aplicaciones que ya hemos instalado. Sin embargo, en módulos anteriores pudimos ver que hay ciertos permisos que se aceptan de forma automática durante la instalación, sin haber posibilidad de gestionarlos más adelante. Por tanto, si queremos una mayor protección es importante conocer herramientas que nos permitan analizar las apps incluso antes de instalarlas. Así podremos tomar decisiones informadas.

Para ello podemos utilizar herramientas como **APKFalcon** y ***Exodus Privacy*****,** que permiten analizar aplicaciones y comprobar los potenciales riesgos que suponen para nuestra privacidad antes de instalarlas. En este módulo final comentamos los aspectos más destacables de cada una de ellas y explicamos su uso a través de un caso práctico. Comenzamos por Exodus Privacy.

1. *Exodus Privacy*

Exodus Privacy es una herramienta que se centra en la transparencia y el control de la privacidad de las aplicaciones móviles.

Haz clic en el icono para acceder a Exodus Privacy

Esta plataforma permite analizar aplicaciones Android para conocer qué datos recopilan y qué rastreadores (*trackers*) incluyen.

Haz clic en el icono para aprender qué son los rastreadores

El proyecto APP-PI es una iniciativa realizada 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)

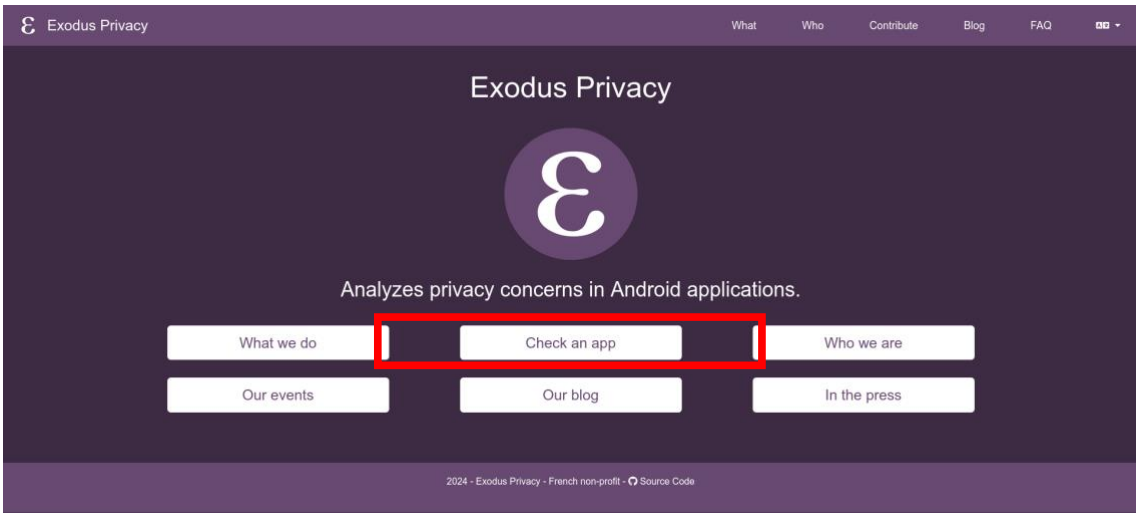
1.1. ¿Cómo funciona Exodus Privacy?

Para utilizar *Exodus Privacy*, podemos ingresar al enlace proporcionado en el apartado anterior y buscar una aplicación específica. La plataforma proporciona un análisis de los permisos que la aplicación solicita, además de un informe sobre los rastreadores que incluye.

La plataforma también permite que los desarrolladores de aplicaciones móviles registren sus apps para que sean analizadas, lo que promueve una mayor transparencia y responsabilidad en el manejo de los datos personales. A continuación, explicamos cómo utilizarla a través de un ejemplo.

1.2. Casos prácticos en Exodus Privacy

Si ingresaste en el enlace (https://exodus-privacy.eu.org/en/), deberías haber accedido a la siguiente página web:



Esta plataforma solo está disponible en inglés o francés. Como se puede observar, en la barra superior se encuentran enlaces a más información sobre ella, aunque aquí nos vamos a centrar en su uso.

Para consultar la información sobre una aplicación, debemos seleccionar la opción "**check an app**", que aparece resaltada en la imagen anterior. Si hacemos clic en esa opción accederemos a la siguiente pantalla. La flecha roja apunta al buscador donde tenemos que ingresar el nombre de las aplicaciones.

El proyecto APP-PI es una iniciativa realizada 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)

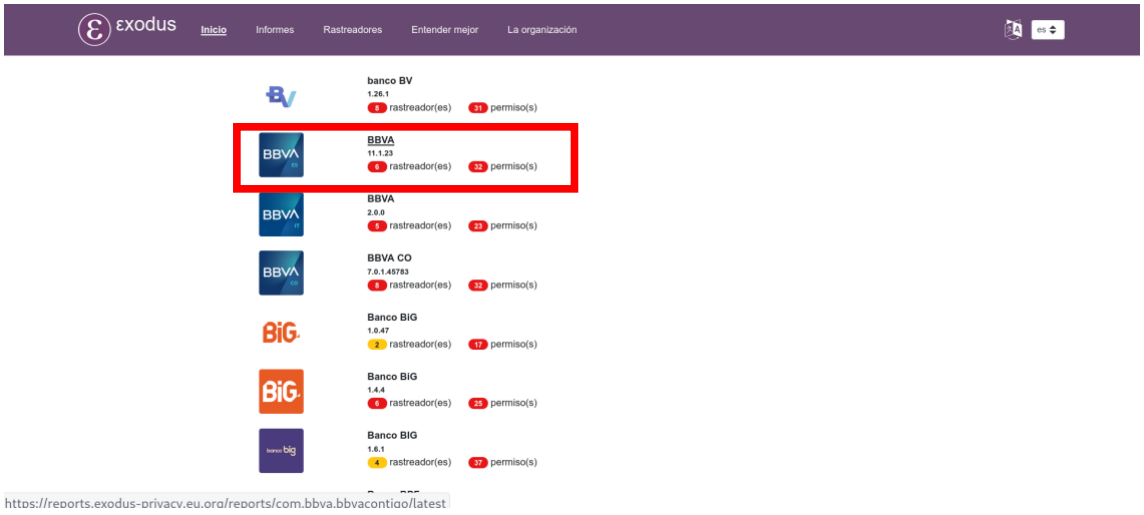
Si continuamos bajando por esa página, observamos que también da las siguientes opciones para saber más sobre rastreadores o ver los últimos informes generados.

En este caso práctico, nos interesa analizar una aplicación, por lo que vamos a volver a subir hacia la parte superior de la pantalla, donde aparece el buscador. Puedes probar a buscar una que sea de tu interés, como puede ser la app de tu banco, por ejemplo. A efectos de esta demostración buscaremos información sobre la del Banco BBVA; para ello escribiremos “Banco BBVA”.

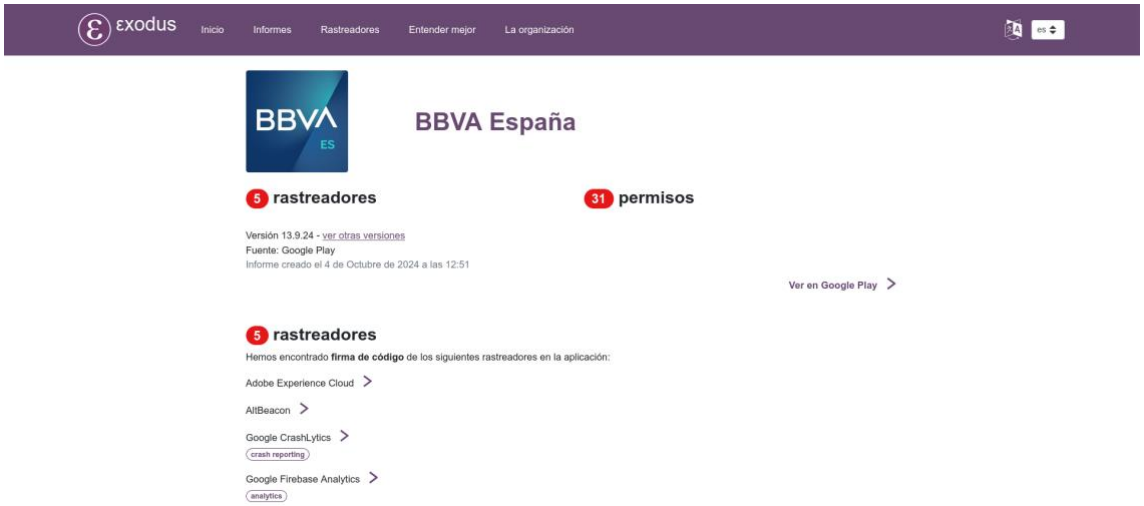
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Tras realizar la búsqueda, observamos que aparecen una serie de resultados diferentes, incluyendo varias versiones de la aplicación de este banco. Seleccionamos aquella que queremos instalar, o ya tenemos instalada en nuestro dispositivo (puedes comprobar tu versión en los Ajustes de tu teléfono, buscando la app en la sección "Aplicaciones").

En este caso hacemos clic en la que aparece resaltada en la imagen siguiente.



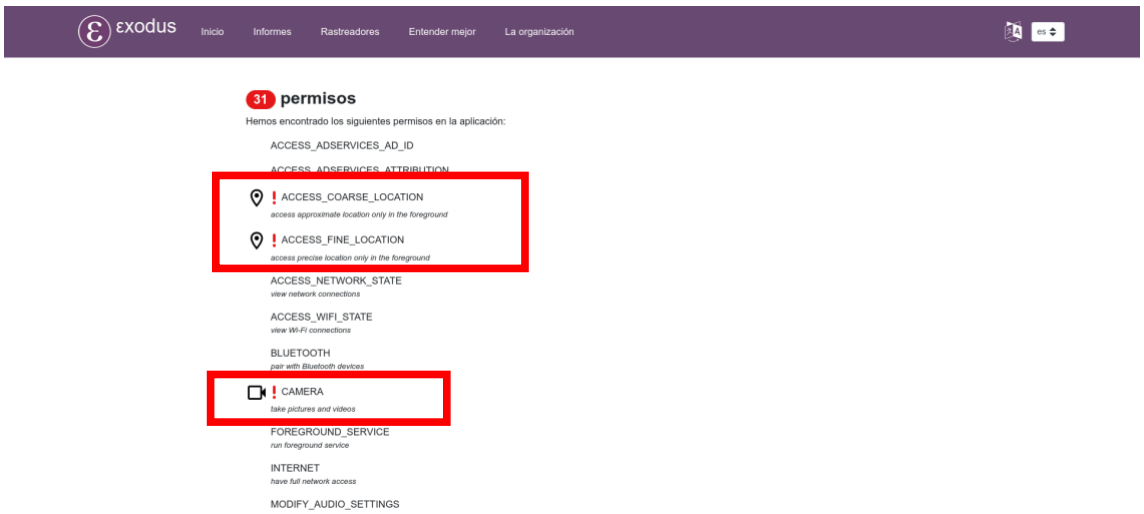
Una vez seleccionada esa opción, nos aparecerá una pantalla como esta:



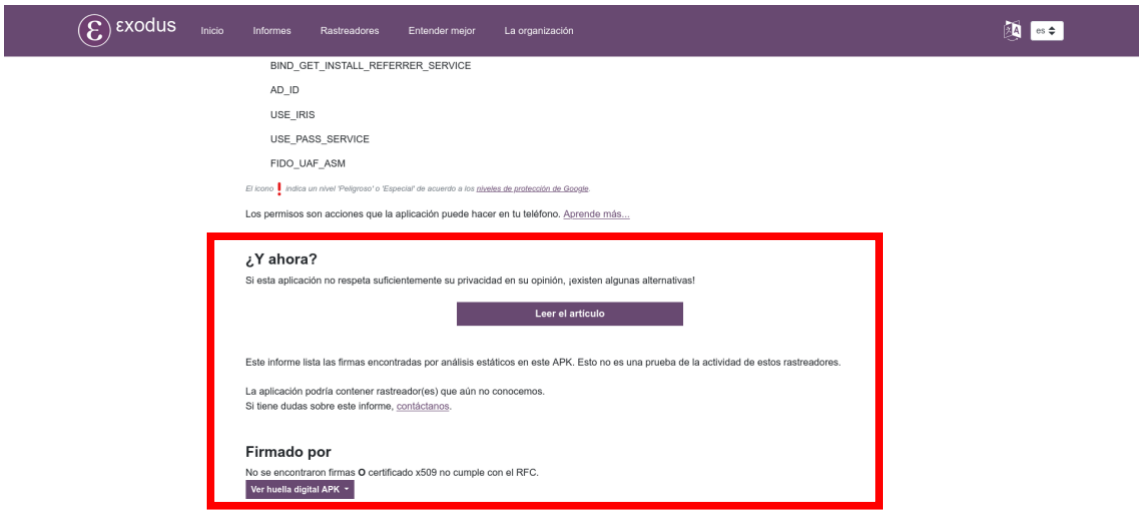
Si continuamos bajando por esa pantalla, encontraremos los permisos que pide esa app. **La plataforma marca con una exclamación los permisos de tipo *dangerous* (de**

El proyecto APP-PI es una iniciativa realizada 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)

tiempo de ejecución), que son los que podemos controlar en los Ajustes de nuestro dispositivo.



Si seguimos bajando aparecerá el nombre de cada uno de los permisos solicitados. Una vez llegamos al fondo aparecen una serie de enlaces que nos permiten acceder a información adicional, como más información sobre los permisos *dangerous*, como se expone en la siguiente captura de pantalla.



Desde aquí te animamos a explorar toda la información que aparece en esta web y a probar con aquellas aplicaciones que más utilices. Así podrás comprobar qué datos personales puedes estar cediendo al realizar actividades digitales en tu día a día.

Como hemos podido ver, Exodus Privacy nos proporciona información sobre los permisos y rastreadores utilizados por una gran variedad de aplicaciones. A continuación, a modo de resumen, exponemos las ventajas que nos reporta el uso de esta plataforma.

El proyecto APP-PI es una iniciativa realizada 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)

1.3. Ventajas de utilizar Exodus Privacy

Transparencia en la recopilación de datos: *Exodus Privacy* nos permite ver de manera clara qué información puede estar recopilando una aplicación, lo que es esencial para tomar decisiones informadas sobre qué aplicaciones instalar.

Identificación de bibliotecas de seguimiento: Al analizar las aplicaciones, *Exodus Privacy* identifica bibliotecas de terceros que pueden estar rastreando nuestra actividad, identifican qué servicios externos están integrados en la app (por ejemplo, de publicidad, análisis o redes sociales) y qué datos pueden estar recolectando, lo que nos ayuda a ser conscientes de cómo se pueden estar utilizando nuestros datos. Cuando instalamos una aplicación, esta no solo puede recopilar datos directamente, sino que también puede incluir **rastreadores**: fragmentos de código de terceros que monitorizan lo que hacemos dentro de la app.

Pero ¿qué es un rastreador? Un rastreador es un componente de software que recopila información sobre el comportamiento del usuario, como qué secciones de la app visita, con qué frecuencia la usa, qué contenido le interesa o incluso su ubicación. Esta información luego se envía a empresas externas, a menudo sin que el usuario sea plenamente consciente de ello.

Un buen ejemplo serían los rastreadores de Google o Meta (Facebook) que incluyen rastreadores de empresas como Google Analytics, Firebase Analytics, Facebook Analytics o Meta Ads. Estos rastreadores permiten a estas grandes tecnológicas seguir el rastro del usuario más allá de una sola app, construyendo un perfil detallado para publicidad personalizada u otros fines comerciales.

Durante el taller del 28 de marzo, uno de los comentarios más reveladores vino de un asistente que, al analizar una app muy común con *Exodus Privacy*, descubrió que contenía más de 10 rastreadores diferentes, muchos vinculados a grandes empresas tecnológicas. Este descubrimiento generó un fuerte impacto: evidenció cómo nuestra actividad digital puede ser monitorizada de forma constante y masiva, incluso cuando usamos aplicaciones que consideramos inofensivas.

El proyecto APP-PI es una iniciativa realizada 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)

Comunidad activa: La web fomenta una comunidad de usuarios interesados en la privacidad, lo que puede contribuir a mejorar el análisis de aplicaciones y compartir información sobre nuevas amenazas y tendencias en el software.

Facilidad de uso: La interfaz de Exodus Privacy es intuitiva y accesible, lo que nos permite comprender los riesgos asociados a las aplicaciones que utilizamos sea cual sea nuestro nivel de experiencia.

Compromiso con la privacidad: Al utilizar Exodus Privacy, apoyamos un enfoque proactivo hacia la protección de nuestra privacidad, lo que contribuye a un entorno digital más seguro y responsable.

Llegados a este punto, continuamos este módulo con una herramienta que, al igual que Exodus Privacy, está diseñada para ayudarnos a entender mejor el comportamiento de las aplicaciones que utilizamos en nuestro día a día. En el siguiente apartado vamos a hablar de APKFalcon, plataforma que proporcionar análisis detallados sobre archivos APK (los paquetes de aplicaciones de Android), ayudándonos a identificar permisos y a entender cómo podemos actuar. Está diseñada para ayudarnos a comprender qué efecto tendrían nuestras decisiones, esas actuaciones en los Ajustes que aprendimos a hacer en el módulo 5.

2. APKFalcon

APKFalcon es una herramienta web que genera un informe sobre los permisos solicitados y los posibles riesgos asociados a las aplicaciones. Esta herramienta es especialmente útil cuando consideramos descargar aplicaciones de repositorios o fuentes alternativas a Google Play Store, ya que nos ayuda a simular qué ocurriría cuando modificamos los permisos que concedemos a una app en los Ajustes. Esto nos permitirá entender mejor qué podemos hacer, y decidir en consecuencia. Todo ello sin comprometer nuestro dispositivo instalando una app que nos pueda parecer demasiado intrusiva. Si somos personas preocupadas por nuestra privacidad cuando usamos nuestros dispositivos, no queremos comprometerlos instalando aplicaciones solo para decidir si las vamos a utilizar.

El proyecto APP-PI es una iniciativa realizada 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)

APKFalcon es un servicio de acceso totalmente abierto. Esta plataforma proporciona un informe con gráficos y métricas sobre el impacto que la aplicación analizada tiene en nuestra privacidad y sobre cómo podemos protegernos **sin necesidad de instalar ninguna aplicación.**

Haz clic en el icono para acceder a APKFalcon

Una ventaja de esta plataforma radica en que nos proporciona la información de forma visual, permitiéndonos apreciar cómo varía el impacto en nuestra privacidad según los grupos de permisos que aceptemos o deneguemos. Entre las formas en las que podemos sacar partido a esta plataforma destaca la comparación de aplicaciones similares, favoreciendo la toma de decisiones informadas que refuercen nuestra privacidad.

2.1. ¿Cómo funciona APKFalcon?

Para utilizar APKFalcon solo necesitamos ingresar en la web y realizar una búsqueda de la aplicación que deseamos analizar (o subir el archivo APK de la misma). Una vez hecho esto, esta herramienta realiza un análisis exhaustivo de los permisos que la aplicación solicita, evaluando cuáles de ellos podrían suponer un riesgo para nuestra privacidad. A continuación, vamos a explicar el funcionamiento de esta herramienta a través de un ejemplo. Te proponemos que sigas la explicación mientras lo compruebas personalmente en su página web (https://apkfalcon.inf.uva.es/).

2.2. Casos prácticos en APKFalcon

Para comenzar, seguiremos el link que se ha proporcionado anteriormente. Este nos llevará a la siguiente web:

El proyecto APP-PI es una iniciativa realizada 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)

Como se puede observar en la imagen anterior, esta nos da la opción de buscar una aplicación a través del nombre de su APK. Incluso, en caso de escribir el nombre de manera incorrecta también nos mostraría el resultado de esta. Para ello, vamos a probar con una de las redes sociales que más se utilizan hoy en día: WhatsApp.

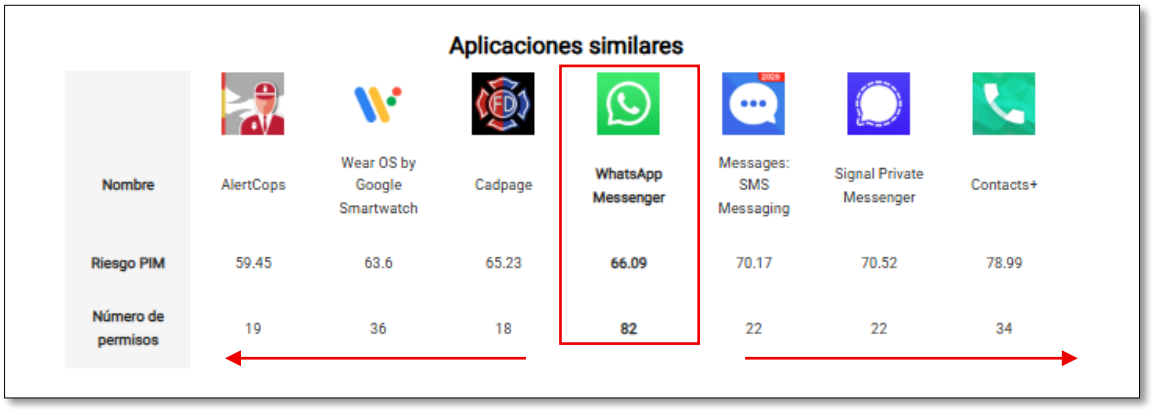
En primer lugar, como ejemplo escribiremos el nombre de forma errónea “wasap”, en el cuadro que aparece en la imagen anterior con el símbolo de lupa.

Una vez hayamos introducido el nombre en el buscador de APK Falcon y hayamos ejecutado la búsqueda, veremos la siguiente pantalla de carga:

Cuando se complete la recuperación de los datos de la aplicación, llegaremos al informe final, pudiendo ver la siguiente pantalla:

Como podemos observar, la web ofrece una métrica que indica el riesgo general que la aplicación supone para nuestra privacidad, así como también su historial de riesgo, tal y como se puede observar en la imagen de abajo.

Mas abajo se muestra una tabla de aplicaciones similares a la que se ha buscado anteriormente y de la cual se ha generado el informe. Como podemos observar en este caso, se muestran tres aplicaciones con un riesgo superior y tres con uno inferior, diferenciando de estas la que hemos buscado porque se encuentra resaltada en negritas.



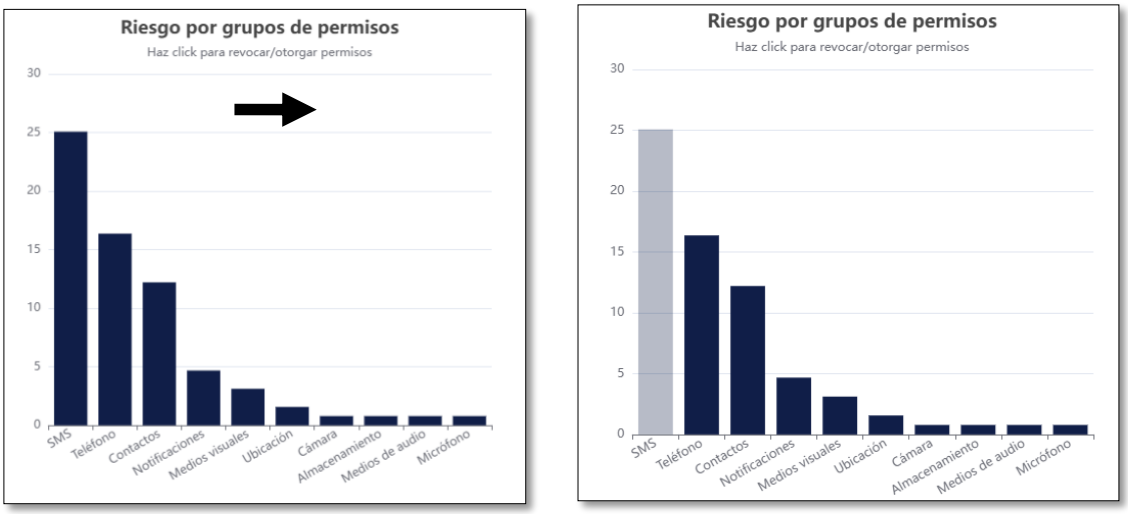
Además, contamos con diferentes gráficos que nos ofrecen información muy variada. A continuación, explicamos en qué consiste cada una de ellas.

En forma de velocímetro tenemos el indicador del riesgo general que esta aplicación supone para nuestra privacidad, siendo en este caso de un **66%**. Cabe destacar que este porcentaje indica que el riesgo de esta aplicación es de **"Riesgo Alto"**, lo que hace ver que esta es una aplicación intrusiva y nos alerta para que comprobemos si los permisos que pide son realmente necesarios.

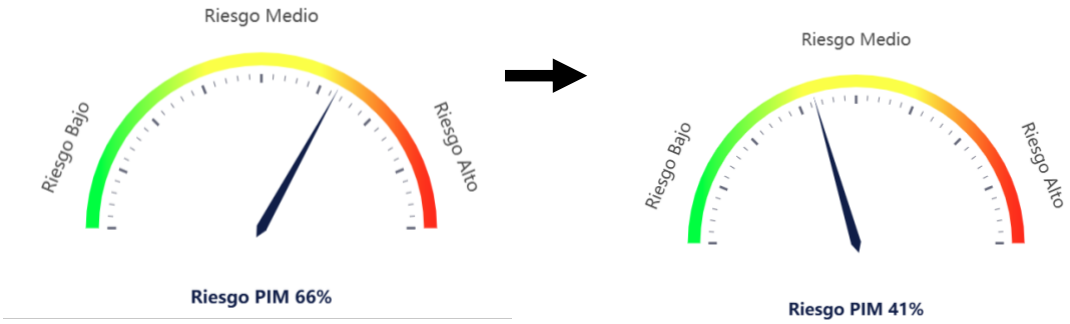
El proyecto APP-PI es una iniciativa realizada al amparo de un convenio de colaboración entre la Universidad de Valladolid y la S.M.E. Instituto Nacional de Ciberseguridad de España M.P., S.A. para la promoción de proyectos estratégicos de ciberseguridad en España, en el marco de los fondos del Plan de Recuperación, Transformación y Resiliencia, financiados por la Unión Europea (Next Generation)

Por otro lado, también tenemos un diagrama de barras que nos indica el riesgo de los permisos. Este es muy interesante, pues nos permite marcar o desmarcar grupos de permisos para ver cómo cambiaría el impacto que estos tienen en nuestra privacidad.

En este caso, a modo de ejemplo, hemos desactivado los permisos de acceso a los SMS.



El resultado ha sido que la aplicación ha pasado de tener un **66%** de riesgo a tan solo un 41%, lo que se ha visto reflejado en el indicador de riesgo general para la privacidad.



Además, todos estos cambios aparecen reflejados en el tercer gráfico que nos proporciona esta plataforma, que nos permite comparar entre el riesgo a la privacidad que suponen diferentes escenarios según los permisos que hayamos concedido. En este ejemplo, han quedado registrados el primer caso (en el que el riesgo era del 33%)

El proyecto APP-PI es una iniciativa realizada 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)

y el segundo (en el que ha pasado a ser un 16%). En la siguiente captura de pantalla podemos ver este resultado.

Finalmente, si bajamos al fondo de la página observaremos que también tenemos la opción “Exportar como PDF”, que nos proporciona un informe completo del impacto a la privacidad que supone esta aplicación, permitiendo así descargar los mismos datos que se han estado consultando, como se puede observar en la imagen de abajo.

Como hemos podido observar, APK Falcon ofrece un análisis detallado y dinámico de las aplicaciones, permitiéndonos identificar no solo los permisos que utilizan, sino también evaluar su impacto sobre nuestra privacidad mediante gráficos interactivos y un índice de riesgo general. Estas funcionalidades la convierten en una herramienta valiosa cuyo empleo favorecerá que tomemos decisiones informadas sobre el uso e instalación de diferentes apps. A continuación, resumimos las principales ventajas que APK Falcon pone a nuestra disposición.

El proyecto APP-PI es una iniciativa realizada 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)

2.3. Ventajas de utilizar APK Falcon

Las principales ventajas que reporta el uso de APK Falcon son:

- **Mayor control sobre los permisos:** APK Falcon ofrece información detallada sobre los permisos solicitados por una aplicación, permitiéndonos evaluar si estos son necesarios para su funcionamiento o si representan un acceso excesivo a nuestros datos personales.
- **Identificación de comportamientos sospechosos:** La herramienta analiza las aplicaciones para detectar posibles amenazas, como malware, spyware o rastreadores intrusivos, ayudándonos a prevenir daños en nuestro dispositivo y a proteger la confidencialidad de nuestra información personal.
- **Facilidad de uso y accesibilidad:** Su diseño intuitivo y fácil de entender permite que cualquier usuario, incluso sin conocimientos técnicos, pueda analizar aplicaciones cargando archivos APK o utilizando URLs de Google Play, obteniendo informes claros y visuales sobre riesgos potenciales.
- **Información visual y práctica:** Los gráficos interactivos y el índice de riesgo general proporcionados por APK Falcon hacen que sea más sencillo interpretar los datos, ayudándonos a comparar diferentes escenarios según los permisos concedidos y tomar decisiones informadas con mayor rapidez.
- **Protección al instalar aplicaciones fuera de tiendas oficiales:** Al optar por descargar aplicaciones desde fuentes externas, aumentamos la exposición a riesgos de seguridad. APK Falcon actúa como una capa adicional de protección, evaluando el riesgo de cada aplicación y alertándonos **antes de su instalación.**

3. Conclusión

En este módulo hemos explorado el uso de Exodus Privacy y APKFalcon, que nos permiten analizar aplicaciones y evaluar los riesgos que las aplicaciones suponen para nuestra privacidad antes de instalarlas. La primera nos ayuda a identificar permisos y rastreadores y la segunda nos ofrece análisis visuales detallados, útiles especialmente para apps de fuentes externas, ayudándonos a evaluar su seguridad y privacidad.

El proyecto APP-PI es una iniciativa realizada 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)

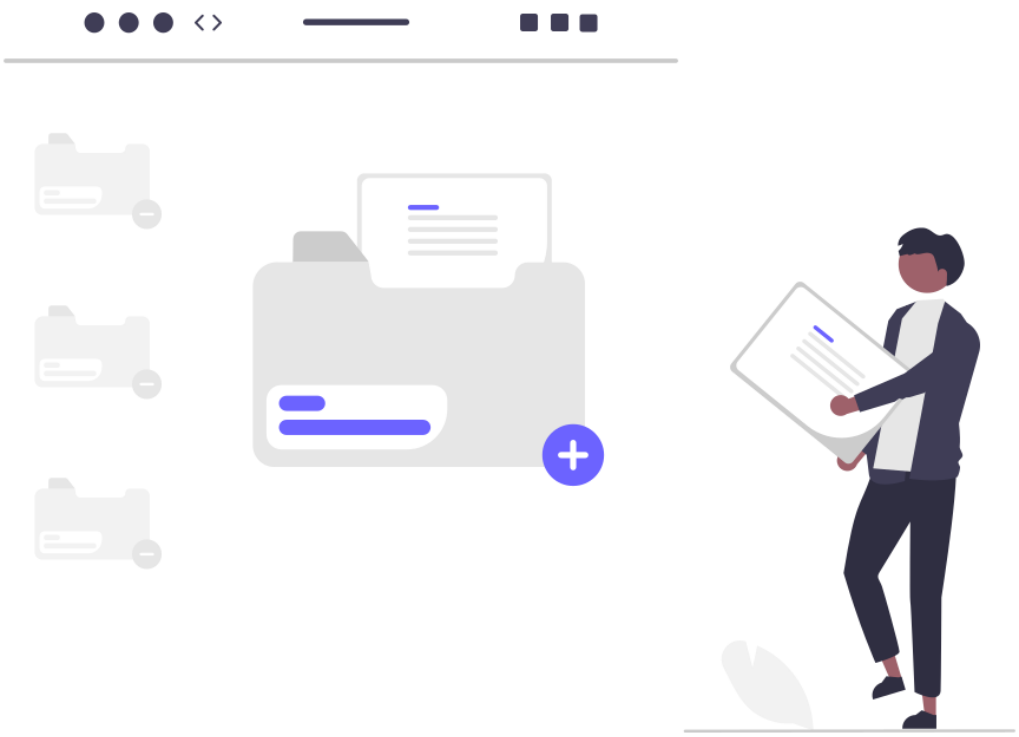
Estas herramientas son fundamentales para reforzar nuestra protección digital, brindándonos el control necesario para gestionar de forma proactiva los datos personales que compartimos. Su uso nos permite adoptar un enfoque más seguro y responsable al interactuar con aplicaciones en nuestra vida diaria.

A lo largo de este curso hemos aprendido cuestiones relativas a nuestra privacidad, desde los marcos legales que protegen nuestros datos personales en el ámbito digital, pasando por los tipos de datos que estamos cediendo a través del uso de dispositivos digitales en nuestra vida cotidiana, continuando por las diferentes formas en las que nuestra privacidad puede verse vulnerada por nuestra actividad en internet y llegando hasta las estrategias que podemos utilizar para protegernos.

Llegados a este punto, puedes comprobar lo aprendido realizando el test. Además, te animamos a ampliar tus conocimientos sobre este tema a través de los materiales complementarios que te ofrecemos.

El proyecto APP-PI es una iniciativa realizada 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)

MATERIALES COMPLEMENTARIOS



Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[13]

Universidad de Valladolid

gi.ingpriv@uva.es

[13]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

Aquí presentamos una recopilación de enlaces que pueden servir para ampliar información. Algunos de ellos están presentes en los módulos, otros no.

Definición de privacidad

- https://dle.rae.es/privacidad

Información sobre los datos personales

¿Qué son los datos personales? Comisión Europea.

Legislación

- Reglamento General de Proyección de Datos (RGPD)
- Ley Orgánica de Protección de Datos Personales y Garantía de los Derechos Digitales (LOPDGDD)

Antivirus populares

Kaspersky

ESET

AVAST

Plataformas

- Exodus Privacy
- APKFalcon

Noticias

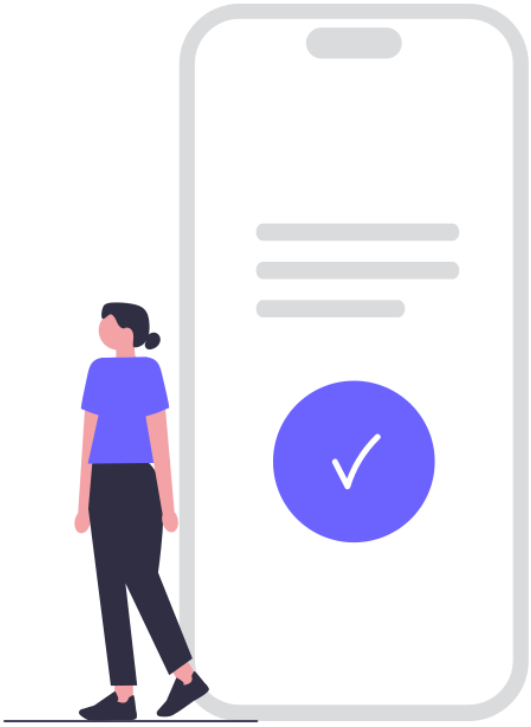
1. "Miles de 'apps' para niños pueden estar violando su privacidad"
2. "Deja de regalar tus datos: hasta un 74 % de las apps piden más permisos de los que necesitan"

El proyecto APP-PI es una iniciativa realizada 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)

3. **“Así recopilan información de tus hijos pequeños a través de las apps“**
4. **“Casi una cuarta parte de las apps móviles recopilan más información del usuario de la que deberían”**
5. **“Google evitó que se publicaran más de dos millones de apps maliciosas en Play Store en 2023“**
6. **“Google reconoce que rastrea a los usuarios de Chrome aunque utilicen el modo 'incógnito'”**
7. **“5 claves para entender el escándalo de Cambridge Analytica que hizo que Facebook perdiera US$37.000 millones en un día”**
8. **“Lo que Snowden ha revelado hasta ahora del espionaje de EE.UU.”**
9. **“Banco Santander sufre un ciberataque que afecta a datos de clientes en España”**
10. **“Así actúa WannaCry, el 'ransonware' que ha atacado a Telefónica y otras grandes empresas españolas”**
11. **“El misterio de las Roomba que publican vídeos íntimos en redes sociales”**

El proyecto APP-PI es una iniciativa realizada 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)

EJERCICIOS



Grupo de Investigación en Ingeniería de la Privacidad de la Universidad de Valladolid[14]

Universidad de Valladolid

gi.ingpriv@uva.es

[14]Equipo del proyecto que colabora en este documento: M. Mercedes Martínez González (IP), Alejandro Pérez de la Fuente, Amador Aparicio de la Fuente, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Quiliano Isaac Moro Sancho, Iván Martín Colomo, Mónica Melero Lázaro, Luis Blanco de la Cruz.

El proyecto APP-PI es una iniciativa realizada 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)

Introducción

Aquí presentamos una serie de ejercicios que resultan útiles para recordar y poner en práctica lo aprendido.

Recordamos que las instrucciones que se dan en los módulos pueden variar según la versión de Android de nuestro dispositivo.

Ejercicio 1

Accede a ***Exodus Privacy*** a través del enlace. Utilizando la información que te proporciona esta plataforma, debes realizar una serie de tareas sobre las siguientes apps:

- Facebook.
- Twitter/X.
- Airbnb.
- La app de tu banco.

1.1. Comprueba el número de rastreadores que utiliza cada aplicación. ¿Crees que suponen un riesgo para tu privacidad? ¿Escribe el por qué?

1.2. Comprueba el número de permisos que utiliza cada aplicación y responde a las siguientes preguntas de manera escrita:

1- ¿Cuáles crees que son de riesgo?

2-De qué permisos habías oído hablar anteriormente.

3- Busca el permiso Read_External_Storage. ¿Qué supone conceder este permiso?

4- Fíjate en la app de tu banco. ¿Por qué crees que necesita permisos como el acceso a contactos o SMS?

5- Basándote en los datos que te da *Exodus Privacy*. ¿Qué aplicación de las analizadas te genera mayor confianza? ¿Cuál menos?

El proyecto APP-PI es una iniciativa realizada 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)

Ejercicio 2

Accede a **Google Play Store** siguiendo el ejemplo mostrado en el módulo 5, busca las mismas aplicaciones que se proponen en el ejercicio 1 y realiza las siguientes tareas:

2.1. Con la información que te proporciona esta tienda, comprueba si al instalar cada aplicación estás dando acceso a los siguientes grupos de permisos:

- Almacenamiento
- Contactos
- SMS
- Localización

2.2. ¿Entiendes la información que te proporciona esta tienda? ¿Confías en esa información? ¿Escribe el por qué?

2.3. Con la información que te da Google Play Store, ¿puedes diferenciar cuáles son los datos recopilados que suponen un mayor riesgo para tu privacidad? Escribe tu respuesta.

2.4. ¿Qué diferencia hay entre datos recopilados y datos compartidos? Escribe tu respuesta.

Ejercicio 3

Entra en la plataforma **APKFalcon** a través del enlace y, fijándote en el ejemplo del módulo 6, busca las mismas aplicaciones que hemos propuesto en el ejercicio 1 y prueba desactivar los permisos.

3.1. Prueba a desactivar los permisos y observa cómo va cambiando la métrica. Comprueba también cómo cambian los diferentes gráficos.

3.2. Comprueba el informe completo que proporciona APKFalcon.

3.3. Compara el impacto sobre la privacidad de las diferentes aplicaciones. ¿Cuál de ellas supone un mayor riesgo para tu privacidad? ¿Cuál supone un riesgo menor? Justifica tu respuesta.

El proyecto APP-PI es una iniciativa realizada 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)

Ejercicio 4

Utilizando tu teléfono móvil Android, accede a la sección de Gestión de Permisos dentro de tus ajustes siguiendo una de las dos vías que hemos explicado en el módulo 5. Elije alguna de las aplicaciones que ya están instaladas y haz lo siguiente:

4.1. Comprueba qué permisos estás concediendo y cuáles no.

4.2. Prueba a desactivar un permiso considerado de tipo *dangerous* (de tiempo de ejecución) por *Exodus Privacy*. ¿Qué funciones pierde la app?

> **Por ejemplo:** Si revocamos el permiso Contactos en la app de nuestro banco, perdemos la capacidad de utilizar Bizum.

4.3. Prueba a cambiar los permisos imprescindibles de "permitir siempre" a "permitir solo cuando se usa la aplicación". ¿Cambia su funcionalidad? ¿Cuál de estas dos opciones te parece más segura? ¿Por qué? Justifica tu respuesta.

4.4. Entra en los permisos de la app de tu banco. ¿Necesita utilizar el micrófono? ¿Por qué? Justifica tu respuesta.

Ejercicio 5

Para reflexionar…

5.1. ¿Qué papel podemos jugar como usuarios para proteger nuestra privacidad?

5.2. ¿Qué medidas podemos tomar para proteger nuestra propia privacidad con las apps móviles?

5.3. ¿A qué riesgos nos exponemos con el uso de aplicaciones móviles?

El proyecto APP-PI es una iniciativa realizada 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)

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).

Equipo investigador:
M. Mercedes Martínez González (IP), Amador Aparicio de la Fuente, Julián Arroyo Álvarez, Alejandro Pérez de la Fuente, Quiliano Isaac Moro Sancho, Margarita Gonzalo Tasis, David Sanz Esteban, Pablo Abel Criado López (Universidad Europea Miguel de Cervantes), Joaquín Adiego Rodríguez, Javier Rodríguez Aparicio, Luis Blanco de la Cruz, Mónica Melero Lázaro, José Andrés González Fermoselle, Ana Isabel Rodríguez Escudero, Víctor Temprano García, Henar Ortega Pérez, Génesis M. De León Alcántara, Mónica Casas Domínguez y Javier Bustos Jiménez.