

Aplicaciones seguras para las mujeres

Las aplicaciones son programas informáticos enfocados en el uso en dispositivos celulares. Como cualquier otro programa que instalas, y dependiendo del objetivo de la aplicación en cuestión, puede requerir acceso al almacenamiento y dispositivos periféricos como la cámara, micrófono, lector de huellas, bluetooth, etc. o datos personales, como nombre, edad, domicilio, etc.

Existen como parte del contexto de las mujeres en el uso de las tecnologías, diversas limitaciones y violencias que se han reproducido, y para erradicarlas es necesaria la participación de actores desde la ingeniería, la academia, el gobierno, las empresas para escuchar activamente a las comunidades de mujeres que se han pronunciado en la defensa de sus derechos digitales.

Las aplicaciones son útiles y prácticas para resolver ciertas necesidades de las mujeres, pero algunas de ellas recaban información del celular y de las usuarias que **puede afectar su derecho a la privacidad**.

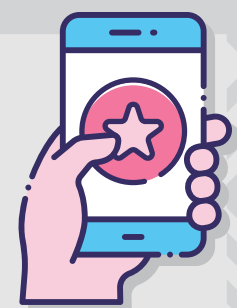
La organización SocialTIC, realizó un “Mapeo y análisis de apps de monitoreo y seguridad para mujeres”, con el objetivo de documentar los permisos, perfiles y funcionalidades de 13 apps enfocadas al uso en contextos de riesgo¹. Algunas conclusiones a señalar:

- Permisos: No son extremadamente invasivas ni requieren permisos incongruentes con su funcionalidad, esto

se extiende a los accesos de geolocalización, cámara y micrófono. Sin embargo, ninguna funciona si no se le otorga permiso a la geolocalización lo cual **no es esencial para su funcionamiento** en algunos casos.

- Gestión de la información: La información que requieren en general es reducida. Y todas **cuentan con políticas de privacidad** ya que es un requisito de las apps de la tienda oficial.
- Funcionalidades: La mayoría cumple las funciones especificadas. Solo círculo menciona manejo de cifrado y otros mecanismos de seguridad, de las demás no existen certezas al respecto. Muy pocas incluyen alguna función de incorporar a alguna autoridad en la alerta. Finalmente, las de cuidados entre pequeñas redes ofrecen mayores funciones y información adicional que puede ser de ayuda, por lo que se perciben como más ágiles para su uso.

Tipos de aplicaciones que más usan las mujeres

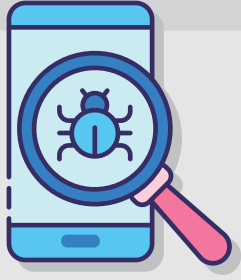


Entre las aplicaciones más descargadas por mujeres se encuentran:

- Redes sociales,
- video-conferencias,
- citas,
- transporte,
- redes de apoyo,
- para encontrar el carro estacionado,
- retoques en fotografías,
- ejercicio,
- seguimiento de la menstruación,
- seguimiento del embarazo,
- pérdida de peso,
- yoga,
- de seguridad,
- geolocalización,
- denuncias, etc.

En los últimos años, debido al auge de la denuncia de diversos actos de violencia contra las mujeres se han desarrollado aplicaciones que buscan dar seguimiento de los recorridos principalmente, para que las mujeres lleguen a salvo a sus destinos, sin embargo, **está lejos de ser una solución** y tampoco es el único enfoque de las aplicaciones dirigidas a mujeres.

Aplicaciones seguras para las mujeres



Entre los riesgos de estas aplicaciones que pueden afectar directamente a las usuarias está:

- Vulneración en la seguridad del sistema.
- Acceso de personas no autorizadas al sistema o a las bases de datos.
- Información no cifrada.
- Venta de los datos recabados.
- Falta de precisión de la información.
- Exposición del historial sexual y de salud.
- Información no cubierta por las leyes de confidencialidad médica.



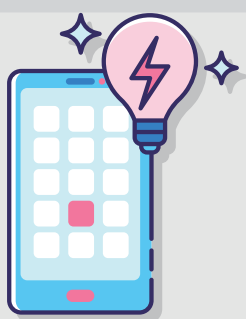
Nuestro cuerpo, nuestros datos

La cantidad de información que las mujeres pueden proporcionar a las empresas tecnológicas por medio de aplicaciones y dispositivos biosensores es muy amplia²:

- **Cuerpo**: dolores, sensaciones, síntomas, ejercicios, horas de sueño, etc.
- **Vagina, útero y vida sexual**: menstruación, posición durante el sexo, color de la sangre, aborto, etc.
- **Emociones**: estrés, ansiedad, falta de concentración, etc.
- **Datos personales**: nombre, teléfono, dirección, correo electrónico, etc.

- **Comportamiento en línea**: Visualización de contenido, páginas visitadas, clics, tipo de dispositivo, etc.
- **Comportamiento fuera de línea**: fiestas, compromisos sociales, etc.

Toda esta información que generan las mujeres -que es solo una parte-, puede ser compartida, vendida a terceros, o en algunos casos vulnerada por la misma empresa de manera irresponsable o por terceros que acceden a las bases de datos de forma ilegal.



Otros algoritmos, otras tecnologías

¿Cómo sería una aplicación feminista?, de acuerdo con la "Guía general para evaluar aplicaciones y servicios digitales"³ de la organización Técnicas Rudas, existen 5 aspectos principales para tomar en cuenta a la hora de evaluar una aplicación y aunque no se enfoca exclusivamente en la evaluación de aplicaciones desarrolladas para mujeres, es un punto de partida:

- **Compromiso con la privacidad**:

Reducción de acceso a tu información:

- ¿Con cifrado controlado por usuarias/os?
- ¿Tiene la opción de configurar autodestrucción de mensajes?

¿Tiene una política de borrado/no almacenamiento de datos y metadatos?

¿Permite el anonimato?

¿Los permisos que pide al instalarse son coherentes con la función de la aplicación?

- **Políticas y marco legal**:

¿Tiene política de privacidad?

¿Es detallada y específica, o general y ambigua?

¿La política de privacidad expresa un compromiso a proteger tus datos a toda costa, o reserva el derecho de compartir tu información, o algo intermedio?

¿Tiene antecedentes de entregar información a gobiernos?

¿En qué país tiene su sede o sus servidores? Son países donde la legislación favorece la privacidad? (pista: UE- sí; EU- no; México- no).

— Compromiso con la seguridad:

- ¿Cifrada en tránsito?
- ¿Cifrado de extremo a extremo?
- ¿Tiene un mecanismo de verificación de identidades?
- ¿Tus datos están cifrados en lugar?
- ¿Existen antecedentes/historial de fallos de seguridad?

— Transparencia:

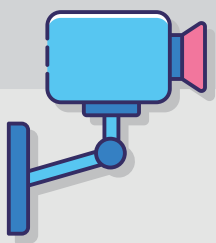
- ¿Publica un informe de transparencia?
- ¿Los informes de transparencia son detallados?
- ¿Responde públicamente con explicaciones sobre fallos de seguridad?
- ¿Ha sido auditada recientemente, y se publicó el informe de auditoría?

— Usabilidad:

- ¿La aplicación es disponible en tu idioma?
- ¿La documentación de la aplicación (políticas, informes, términos y condiciones, tutoriales, explicaciones técnicas) está disponible en tu idioma?
- ¿Es compatible entre diferentes sistemas operativos y modelos de dispositivos?
- ¿Tiene buena reputación desde la experiencia de las usuarias?

— Perspectiva política:

- ¿Diseñado con perspectiva de género?
- ¿Código abierto?
- ¿Software libre?
- ¿Modelo de negocio?
- ¿Compañía/colectivo que lo desarrolla?



Vigila y controla tus aplicaciones

Existen también formas en que podemos reducir el control de las aplicaciones que se instalan. Aunque requiere tiempo para comprender el funcionamiento y las alternativas, existen herramientas y tácticas que podemos usar para manejar nuestra privacidad.

La decisión es de cada una, pero la guía anterior puede ayudar a tener en mente esas consideraciones y evaluarlas con el paso del tiempo para tener un mejor control sobre la identidad digital de cada una.

Por otro lado, existen herramientas que ayudan a estas tareas de control sobre las aplicaciones como **Exodus-privacy**⁴, que es una plataforma de auditoría de

privacidad para aplicaciones Android, analiza las aplicaciones en busca de rastreadores embebidos (códigos destinados a recopilar información sobre la persona que utiliza la aplicación, sobre cómo la utiliza o sobre el teléfono inteligente que se está utilizando) en estas, y lista además los permisos (geolocalización, contactos, archivos, micrófono, cámara, etc.) que cada una solicita, posibilitándole en la muchos casos deshabilitarlos y habilitarlos con mayor control.

Aunque también tanto Android como iOS ofrecen la posibilidad de administrar los permisos que cada aplicación utiliza⁵:



Desde la versión 6.0 de Android es posible administrar los permisos de las aplicaciones. Esta información puede encontrarse en **Configuración > Aplicación > Permisos**.



Apple iOS, ofrece un panorama amplio sobre los permisos que tienen las aplicaciones de acceder a diferentes tipos de datos. Esta información puede encontrarse en **Configuración > Privacidad**.

En general puedes desactivar los permisos para el seguimiento de datos cuando las aplicaciones no están en uso, por ejemplo, las aplicaciones de rutas y mapas no necesitan

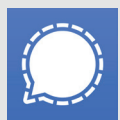
tener acceso a los datos de tu ubicación cuando no los estás usando activamente.

Recomendaciones⁶

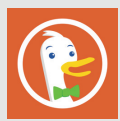
Como en la seguridad digital, que es un proceso largo y colectivo, es necesario seguir informándose sobre las herramientas digitales, las políticas de privacidad, las legislaciones, las vulnerabilidades, etc; y compartirlas con tus círculos para **socializar tanto las dudas como las certezas**.

Acercarse a las organizaciones que dan seguimiento a estos temas, en la medida de las posibilidades de cada una, para mantenerse al día, e incluso poder contribuir sitúa a las **usuarias como sujetas activas en dichas tecnologías** que pueden lograr cambios significativos para todas.

Utiliza aplicaciones que **tomen en cuenta tu privacidad** y que establezcan claramente en sus políticas de privacidad qué información recopilan para su funcionamiento y que aclaren si la información es o no compartida con terceros.



Signal es una aplicación de mensajería segura que utiliza cifrado de extremo a extremo para proteger textos y llamadas de voz.



DuckDuckGo es un motor de búsqueda que explícitamente no recopila, almacena o comparte ninguna información sobre sus usuarias.



Disconnect también es una aplicación que busca proteger a las usuarias del rastreo y mejorar el rendimiento del dispositivo.

Realiza un mantenimiento regular de las aplicaciones instaladas, actualízalas regularmente, comprueba cada vez los permisos a los que acceden, y elimina las aplicaciones que no utilizas. Las actualizaciones suelen venir con parches de seguridad, mejoras y características nuevas, por lo que pueden acceder a diferentes datos y de diferentes maneras cada vez que se actualizan. Además algunas también recopilan datos **cuando están inactivas** por lo que podría ser de consideración removerlas si no han sido utilizadas en más de un mes y pueden volver a instalarse en el futuro.

Desactiva los permisos de las aplicaciones mientras no están en uso, así **también se ahorra energía** de la batería.

Finalmente, puedes revisar Círculo: Stay Safe Together, y revisar la presentación de la aplicación en Beta⁷.



Círculo: Stay Safe Together

Referencias

- 1 SocialTIC, "Mapeo y análisis de apps de monitoreo y seguridad para mujeres". Disponible en: <https://socialtic.org/wp-content/uploads/2019/11/Mapeo-y-ana%CC%81lisis-de-herramientas-de-seguridad-para-mujeres-2.pdf>
- 2 Chupadados, MENSTRUAPPS - Cómo convertir tu menstruación en dinero (para los demás). Disponible en: <https://chupadados.codingrights.org/es/menstruapps-como-transformar-sua-menstruacao-em-dinheiro-para-os-outros/>
- 3 Técnicas Rudas. Guía general para evaluar aplicaciones y servicios digitales. Disponible en: <https://share.mayfirst.org/s/yxB9TsozWqJPxXx>
- 4 exodus. La plataforma de auditoría de privacidad para aplicaciones Android. Disponible en: <https://reports.exodus-privacy.eu.org/en/>
- 5 Slate Magazine. How to Understand What Info Mobile Apps Are Collecting About You. Disponible en: <https://slate.com/technology/2017/02/how-to-understand-what-info-mobile-apps-collect-about-you.html>
- 6 Slate Magazine. How to Understand What Info Mobile Apps Are Collecting About You. Disponible en: <https://slate.com/technology/2017/02/how-to-understand-what-info-mobile-apps-collect-about-you.html>
- 7 The Guardian Project. Círculo, presentación de la aplicación en Beta. Disponible en: https://docs.google.com/presentation/d/1PjBQ2Zub7aF-Saef98HETSy5xFzFP21kik_zyi3wB8Hw/edit#slide=id.g33c4d9b5a0_0_180