Aplicaciones que espían: qué permisos le das a tu móvil (y por qué importa más de lo que crees)

Tu teléfono sabe más de ti que tú mismo. La pregunta es a quién se lo está contando.

Introducción: El espia que llevas en el bolsillo

Hay una pregunta que muy poca gente se hace cuando descarga una app nueva: **¿por qué necesita esto acceso a mi micrófono?**

No lo preguntamos porque el proceso está diseñado para que no lo hagamos. Aceptas, sigues, y en diez segundos ya estás usando la aplicación. Lo que no ves es lo que ocurre justo después: una cadena silenciosa de accesos, lecturas y transmisiones de datos que no has autorizado conscientemente, aunque técnicamente hayas pulsado "aceptar".

No hablamos de ciencia ficción ni de teorías conspirativas. Hablamos de un modelo de negocio consolidado, legal en muchos casos, y extraordinariamente rentable: **la economía de los datos personales.** Y tu móvil es el punto de acceso más rico que existe a esa economía.

Lo más preocupante no es que las apps recopilen datos. Es que lo hacen con información que va mucho más allá de lo que necesitan para funcionar, y que esos datos —tus datos— acaban alimentando perfiles de comportamiento que se compran, se venden y, en el peor de los casos, se filtran o se explotan.

Este artículo no es un manual de paranoia digital. Es una guía para entender qué estás cediendo, por qué algunos permisos son completamente innecesarios, y cómo puedes auditarlo hoy mismo en menos de cinco minutos.

Qué son realmente los permisos y qué habilitan

Cuando una aplicación solicita acceso a algo de tu teléfono —tu cámara, tu ubicación, tus contactos— está pidiendo una llave. Una llave que, una vez concedida, puede usar cuando quiera, no solo en el momento en que tú la necesites activamente.

Eso es lo que mucha gente no comprende: los permisos no son contextuales por defecto. Una app a la que le diste acceso al micrófono en 2023 para hacer videollamadas puede seguir escuchando actualmente en segundo plano, aunque no la tengas abierta. Técnicamente, los sistemas operativos modernos han mejorado mucho en esto —Android e iOS limitan cada vez más el acceso en segundo plano—, pero el margen de exposición sigue siendo considerable.

Los permisos más sensibles son, por este orden: **ubicación, micrófono, cámara, contactos, almacenamiento y actividad física.** Cada uno de ellos, en manos equivocadas o combinados entre sí, permite construir un perfil enormemente detallado de quién eres, dónde estás, con quién te relacionas y cómo te comportas.

Esto tiene un nombre en el ámbito de la inteligencia: **OSINT pasivo enriquecido.** No hace falta hackear nada. Solo hace falta que hayas instalado la app equivocada y pulsado "aceptar" sin leer.

Por qué una linterna no necesita tu micrófono

El ejemplo es antiguo pero sigue siendo el más clarificador. Hubo una época, no muy lejana, en la que apps de linterna solicitaban acceso a la ubicación GPS, a los contactos y al micrófono. Ninguno de esos permisos tiene relación funcional con encender el flash de tu cámara. Cero.

¿Por qué lo pedían entonces? Porque el modelo de ingresos no era la linterna. Era los datos. La app era gratuita, tú eras el producto.

Hoy ese patrón se ha sofisticado. Ya no son solo apps obviamente prescindibles. Son **aplicaciones de productividad, juegos casuales, teclados alternativos, apps de edición de fotos y herramientas de clima** las que acumulan permisos que no necesitan para su función declarada.

Un teclado de terceros que solicita acceso completo a tu actividad en pantalla tiene, en principio, la capacidad técnica de registrar todo lo que escribes: contraseñas, mensajes privados, búsquedas médicas, conversaciones íntimas. Esto no significa que lo haga. Pero la posibilidad existe, y en muchos casos ni los términos y condiciones lo descartan explícitamente.

La regla que deberías aplicar es simple y no requiere conocimientos técnicos: **si no entiendes por qué una app necesita ese permiso para hacer lo que dice hacer, no se lo des.** Y si ya se lo diste, es hora de revisarlo.

El permiso que más se subestima: la ubicación en segundo plano

De todos los permisos disponibles, el de ubicación permanente —lo que los sistemas operativos llaman "siempre" o "en segundo plano"— es probablemente el más invasivo y el menos cuestionado.

Saber dónde estás en tiempo real, durante semanas o meses, no es solo saber dónde estás. Es saber dónde vives, dónde trabajas, a qué médico vas, qué bares frecuentas, con quién te reúnes y cuándo te vas de vacaciones. Es, en esencia, un mapa completo de tu vida.

Este tipo de datos se comercializa activamente en plataformas de *data brokers*: empresas cuyo negocio es agregar, cruzar y vender perfiles de comportamiento a anunciantes, aseguradoras, fondos de inversión o cualquier empresa dispuesta a pagar por ellos. Nada de esto es ilegal en la mayoría de jurisdicciones. Todo es fruto de ese "aceptar" que hiciste sin leer.

Para familias con hijos adolescentes, el riesgo se amplifica. Las apps de redes sociales, juegos móviles y plataformas de entretenimiento orientadas a menores son algunas de las que históricamente han recopilado datos de ubicación de forma más agresiva. Conocer ese riesgo y actuar en consecuencia es parte de la responsabilidad digital parental.

Cómo auditarlo en 5 minutos: pasos concretos

No necesitas instalar nada ni ser técnico. Solo necesitas entrar en los ajustes de tu teléfono y saber qué mirar.

En iPhone (iOS): Ve a *Ajustes → Privacidad y seguridad*. Desde ahí puedes revisar permiso por permiso —ubicación, micrófono, cámara, contactos— y ver exactamente qué apps tienen acceso y en qué condiciones. La sección de *Informes de privacidad de las apps* te muestra, además, con qué frecuencia cada app ha accedido a tus datos en los últimos siete días.

En Android: Ve a *Ajustes → Privacidad → Gestor de permisos*. Allí verás, agrupado por tipo de permiso, qué aplicaciones tienen acceso a cada recurso. Presta especial atención a las que tienen acceso "siempre" a la ubicación o acceso al micrófono sin ser apps de comunicación.

Al revisar, hazte tres preguntas por cada app: ¿Uso esta aplicación regularmente? ¿Necesita este permiso para funcionar? ¿Confío en la empresa que la desarrolla? Si la respuesta a cualquiera de las tres es no o no lo sé, revoca el permiso o desinstala directamente.

Un criterio complementario: **las apps que no has abierto en más de 30 días merecen una revisión especial.** Las versiones recientes de iOS y Android pueden revocar permisos automáticamente en apps inactivas, pero no siempre ocurre, y no siempre cubre todos los permisos.

El problema más profundo: los datos que no parecen datos

Hay una dimensión de este problema que va más allá de los permisos visibles. Cuando una app accede a tus contactos, no solo conoce tu nombre y tu número: conoce el nombre, el número y el tipo de relación de cada persona que tienes guardada. Cuando accede a tu calendario, sabe con quién te reúnes y sobre qué. Cuando lee tus fotos, en muchos casos también lee los metadatos de cada imagen: fecha, hora y **coordenadas GPS exactas** de dónde fue tomada.

Los datos que parecen inocuos individualmente se convierten en algo completamente diferente cuando se cruzan entre sí. Esto es lo que los analistas de inteligencia llaman **correlación de fuentes abiertas**, y es exactamente lo que hacen los sistemas de perfilado de datos con la información que les cedes a través de las apps.

Para la ingeniería social —el tipo de ataque que más crece en 2026, como vimos en el artículo anterior de este blog— este tipo de información es oro puro. Un atacante que sabe dónde vives, a qué empresa perteneces, quiénes son tus contactos más frecuentes y cuál es tu rutina diaria tiene todo lo que necesita para construir un engaño que parezca legítimo desde el primer segundo.

Reflexión estratégica: la privacidad no es comodidad sacrificada, es higiene digital

Existe una narrativa muy extendida que presenta la privacidad digital como una renuncia a la comodidad. "Si quieres usarlo gratis, pagas con tus datos." Esa afirmación no es necesariamente falsa, pero sí está incompleta.

Lo que no se dice es que la mayoría de los permisos que ceden estas apps no son necesarios para la experiencia de uso. Una app de clima no necesita tu micrófono para darte la previsión del tiempo. Un juego casual no necesita tu ubicación exacta para que puedas jugar. El acceso excesivo a datos no mejora el servicio: **mejora el perfil comercial que se construye sobre ti.**

Entender esto cambia el marco. No estás eligiendo entre comodidad y privacidad. Estás eligiendo cuánto control quieres tener sobre una información que tiene valor real —económico, estratégico y de seguridad— y que, una vez cedida, no puedes recuperar.

La higiene digital no es paranoia. Es el equivalente en el mundo digital de no dejar las llaves de tu casa colgadas en la puerta.

Tu próximo paso (y son solo 5 minutos)

Hoy mismo, antes de cerrar este artículo, puedes hacer tres cosas: entra en los ajustes de privacidad de tu teléfono y revoca el acceso al micrófono y la ubicación de todas las apps que no sean de comunicación o mapas, desinstala las apps que no hayas usado en el último mes, y revisa si alguna de las apps que tienes instaladas tiene acceso "siempre" a tu ubicación sin que lo hayas decidido conscientemente.

Si tienes hijos con smartphone, haz este ejercicio con ellos. No como vigilancia, sino como educación: mostrarles qué está ocurriendo con sus datos es una de las formas más concretas de cultura digital que puedes transmitirles.

Si este artículo te ha resultado útil, compártelo con alguien que uses el teléfono sin pensar en esto. La privacidad digital se construye con decisiones pequeñas, tomadas a tiempo. Visita el blog para acceder a más recursos gratuitos sobre seguridad digital aplicada.

Isaac Ruiz Romero