BID
Banco Interamericano de Desarrollo

Tecnologías digitales para la notificación de exposición en época de pandemia

Ignacio Cerrato
Marcelo D´Agostino
Gemma Galdon Clavell
Cristina Pombo
Luis Tejerina

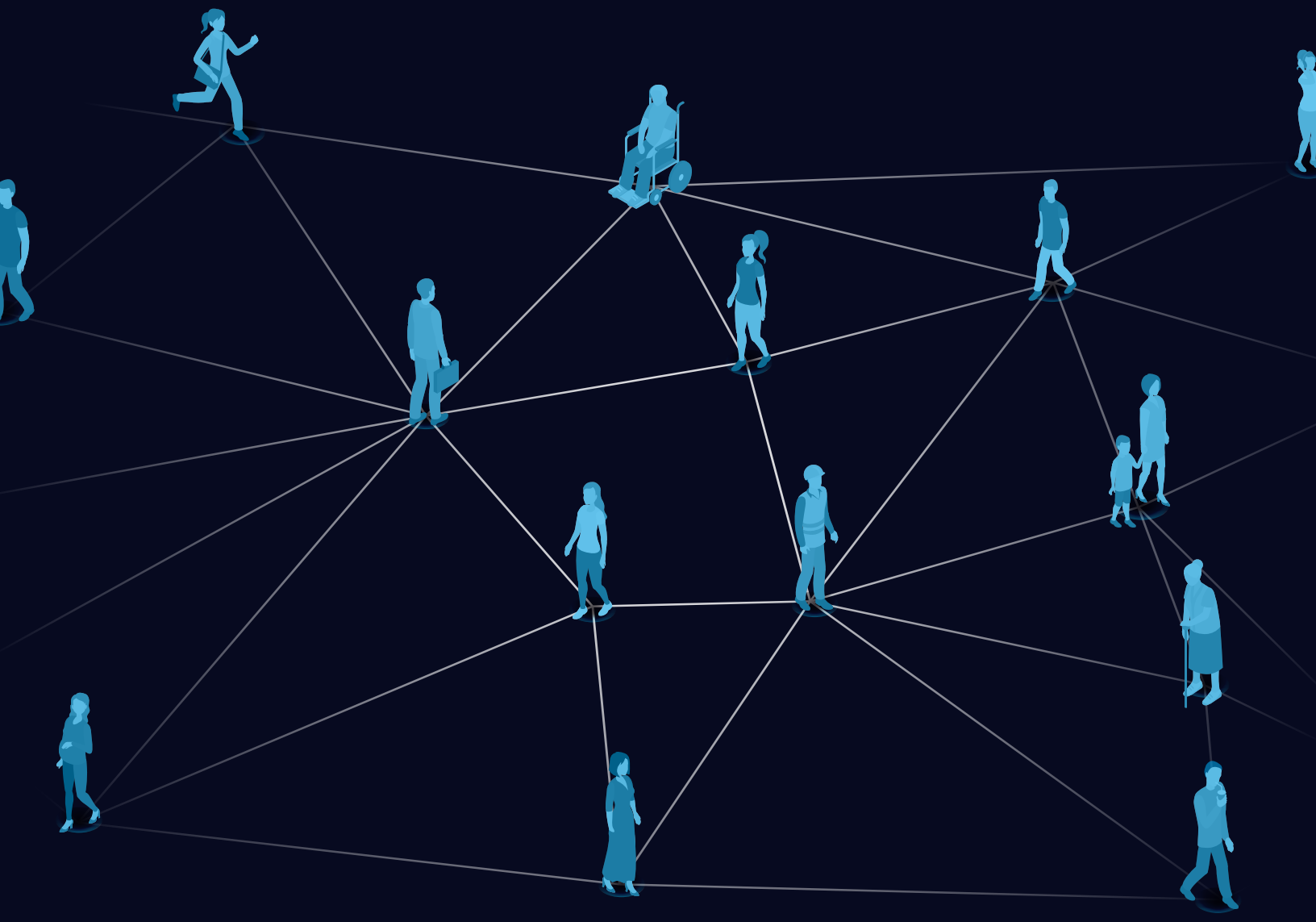
Sector Social
División de Salud y Protección Social
Departamento de Tecnología de la Información

DOCUMENTO PARA DISCUSIÓN Nº
IDB-DP-00836

Diciembre 2020

Tecnologías digitales para la notificación de exposición en época de pandemia

Ignacio Cerrato, Marcelo D´Agostino, Gemma Galdon Clavell, Cristina Pombo y Luis Tejerina



Tecnologías digitales para la notificación de exposición en época de pandemia*

Ignacio Cerrato, Marcelo D´Agostino, Gemma Galdon Clavell, Cristina Pombo y Luis Tejerina[1]

Introducción

El rastreo de contactos es el proceso de detectar, evaluar y decidir qué hacer con las personas que se han visto expuestas a una determinada enfermedad contagiosa con el fin de evitar que la transmisión se extienda[2]. La pandemia causada por la COVID-19 ha desbordado la capacidad de los equipos dedicados a esta tarea generando la necesidad de nuevas técnicas y herramientas para asistir en este proceso.

El tiempo de respuesta de los gobiernos ante una emergencia como la actual es vital para la contención y protección de vidas, y las lecciones aprendidas durante el año 2020 son claves para comprender cómo las tecnologías pueden ayudar a combatir enfermedades infecciosas. Este documento conjunto del Banco Interamericano de Desarrollo (BID) y la Organización Panamericana de la Salud (OPS) pretende mostrar cómo las tecnologías pueden ayudar a los gobiernos a superar crisis de esta categoría. En él se recopilan y analizan las distintas soluciones puestas en marcha con el objetivo de ayudar a distintos tipos de organizaciones o gobiernos a planear sus estrategias de rastreo de contactos y se incluyen recomendaciones con base en las experiencias existentes.

Las enfermedades altamente infecciosas son difíciles de contener, especialmente aquellas que tienen bajas tasas de mortalidad y en las que se dan casos asintomáticos. Esta última característica hace que los individuos contagiados continúen con su vida sin saber que están transmitiendo la infección. Sin embargo, aun considerando que la tasa de mortalidad pueda ser baja en comparación con otras enfermedades, al afectar a gran parte de la población, miles, e incluso millones, de vidas se encuentran en riesgo.

1 Los autores agradecen los valiosos comentarios y aportes de Myrna Marti, Francesc Saigí Rubió, Daniel Otzoy, Alexandre Bagolle y Alejandra Holguín.

2 OMS (2020) El rastreo de contactos en el marco de la COVID-19. Orientaciones provisionales

La primera respuesta de muchos países y gobiernos ante la actual pandemia de COVID-19 ha sido la de decretar cuarentenas preventivas con diferentes tipos de restricciones a la socialización y el intercambio para los ciudadanos. Su principal ventaja es que permite que las personas contagiadas no transmitan la enfermedad durante el periodo infeccioso. Sin embargo, requieren por parte del gobierno y de los ciudadanos un gran esfuerzo que es difícil de sostener en el tiempo, y conlleva otras importantes consecuencias sobre la salud, la sociedad y la economía.

El rastreo manual de contactos, seguido de las cuarentenas, es y ha sido históricamente una de las medidas clave en la contención de cadenas de contagio. Implica que quienes dan positivo en una enfermedad infecciosa sean entrevistadas por personal cualificado para identificar a aquellas personas con las que han interactuado en el período previo al resultado de la prueba. Estas personas son entonces contactadas y alertadas del riesgo en el que se encuentran, y se toman las medidas oportunas (cuarentena, test, seguimiento estricto). En este sentido, el rastreo de contactos se convierte en un pilar clave para interrumpir la cadena de transmisión de una enfermedad infecciosa y, por lo tanto, representa un instrumento esencial de salud pública para controlar los brotes epidémicos infecciosos[3].

Así pues, las **tareas principales** de los rastreos de contactos son[4]:

1. **Identificación de los contactos:** una vez que se confirma que alguien está contagiado por un virus, se investigan las actividades del mismo y las actividades y funciones de quienes le han rodeado desde el inicio de la enfermedad. Se considera contacto cualquiera que haya estado cerca de la persona contagiada.

2. **Elaboración de una lista de contactos:** se prepara un listado en el que han de aparecer todas aquellas personas que se considere que han tenido contacto con la persona contagiada. Se debe intentar identificar a todos los incluidos en la lista e informarles de que están clasificados como contactos, de lo que ello implica, de las medidas que se tomarán a continuación y de la importancia de que reciban una atención inmediata en caso de que presenten signos y síntomas. Asimismo, deben recibir información sobre las formas de prevenir la enfermedad. En algunos casos, los contactos de alto riesgo pueden necesitar cuarentena o aislamiento, en su domicilio o en el hospital.

3. **Seguimiento de los contactos:** se realiza un control regular de todos los contactos para detectar síntomas y signos de infección.

La COVID-19 está siendo un catalizador del uso de tecnología en frentes muy diversos y propició que se implementaran una serie de soluciones digitales que han servido como complemento al rastreo manual de casos. Una de ellas son las apps para el rastreo digital de interacciones. Esta herramienta **en ningún caso sustituye al rastreo manual**. El uso de *apps* de rastreo de interacciones tampoco permite prescindir de otras medidas como el distanciamiento social o los hábitos de higiene, como el lavado de manos o uso de alcohol en gel. Solo combinando todas las precauciones posibles se consigue detener la cadena de contagios.

3 Idem.

4 OMS (2017). Rastreo de los contactos en situaciones de brotes epidémicos. Preguntas y respuestas en línea

Estas herramientas han sido implementadas por los gobiernos de muy diversas formas ante la pandemia. Por una parte, surgieron iniciativas públicas nacionales y subnacionales centralizadas para contener la enfermedad dirigidas a todos los ciudadanos y que, en algunos países, eran obligatorias. Por otra parte, en aquellas naciones donde el gobierno no dio una respuesta centralizada hay soluciones privadas, organizadas por empresas, universidades u otras organizaciones que necesitan hacer su propio rastreo de contactos (por ejemplo, utilizando pequeños dispositivos que alertan a los trabajadores en una empresa si no están cumpliendo con las reglas de distanciamiento social).

Las apps para rastreo de contactos no representan una sustitución al rastreo manual ni permiten prescindir de otras medidas como el distanciamiento social o los hábitos de higiene, como el lavado de manos. Sólo combinando todas las precauciones posibles se consigue parar la cadena de contagios.

Tecnologías disponibles

Todas las soluciones disponibles se basan en el mismo concepto de emitir y analizar señales radioeléctricas para obtener información sobre la posición y/o cercanía con otras personas. La habilidad para tener mediciones confiables es vital para evitar falsos positivos que son sumamente costosos para los equipos de rastreo de contactos. La escalabilidad de estas soluciones depende de la facilidad o dificultad para distribuir los dispositivos necesarios para obtener dicha información, siendo el costo de adquisición y distribución de dichos dispositivos lasmayores barrera.

Dispositivos portátiles o Wearables

Entre estas soluciones se encuentran aquellos dispositivos que las personas deben llevar consigo para emitir y recibir señales. Este tipo de soluciones son viables en grupos acotados, como pueden ser los empleados de una empresa, los estudiantes de una universidad o el personal de un hospital.

Si bien algunos gobiernos, como el de Singapur, están trabajando en este enfoque (Trace Together), resulta limitado para aquellos grupos de población que necesiten una solución confiable y simple, como las personas de edad avanzada.

Las señales más populares usadas en estos dispositivos son, principalmente dos:

- **BLE** (Bluetooth Low Energy): Basada en el protocolo de señal *Bluetooth* utilizado para enviar información entre dispositivos, BLE emite señales que periódicamente son recibidas por otros dispositivos cercanos. La precisión es la mayor limitante de esta tecnología, ya que usa la fuerza de la señal RSSI (*Received Signal Strength Indicator*) para calcular la proximidad. El RSSI puede verse afectado por factores ambientales, como la forma del espacio o la presencia de agua o metales. Si bien es difícil decir cuál es el rango de error promedio, se habla que puede oscilar entre los uno o dos metros.

- **UWB** (*Ultrawide Band*): Se trata de una señal similar a la BLE, con la diferencia de que para calcular la proximidad utiliza el "tiempo de vuelo" de la señal. De esta manera la señal es menos susceptible a factores ambientales que deterioran su fuerza, aunque sí puede verse afectada por la presencia de cuerpos u objetos entre los dispositivos. En condiciones normales, el margen de error se encuentra entre los 10 y los 15 centímetros. UWB es una tecnología usada principalmente en aplicaciones militares, y desde 2002 ha crecido rápidamente para aplicaciones privadas como posicionamiento interno.

Aplicaciones móviles

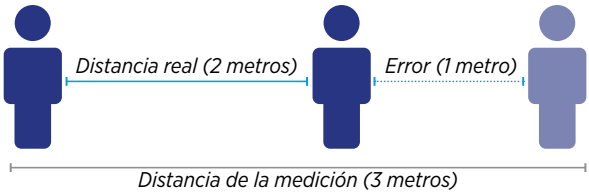
En situaciones en las que es complejo o poco práctico entregar un nuevo dispositivo a las personas que participaran en el programa, se intenta utilizar dispositivos que ya estén en uso.

La solución más popular en grandes poblaciones consiste en emplear aplicaciones móviles que pueden ser instaladas en los teléfonos inteligentes de los usuarios. Estos dispositivos móviles ofrecen grandes posibilidades de interacción con su entorno que hasta el momento han sido utilizadas para múltiples funciones. Funcionan notificando a los usuarios si alguien con quien han estado en contacto ha dado positivo con posterioridad a su interacción.

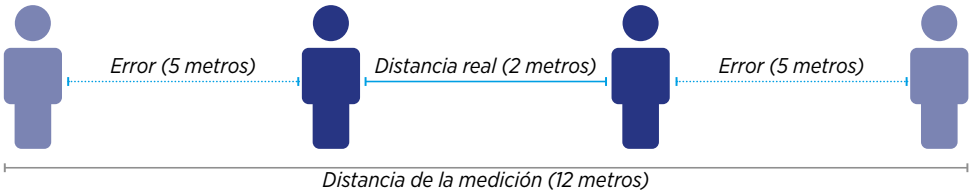
Estas aplicaciones usan los sensores de los teléfonos para detectar contactos. Los sensores pueden ser *Bluetooth*, GPS o Wifi, aunque los dos últimos han sido descartados debido a su baja precisión. Su principal ventaja es que son escalables y la inversión es relativamente baja ya que los dispositivos ya están en uso.

La gráfica siguiente considera el máximo error posible en cada caso, entendiendo que puede variar según las condiciones.

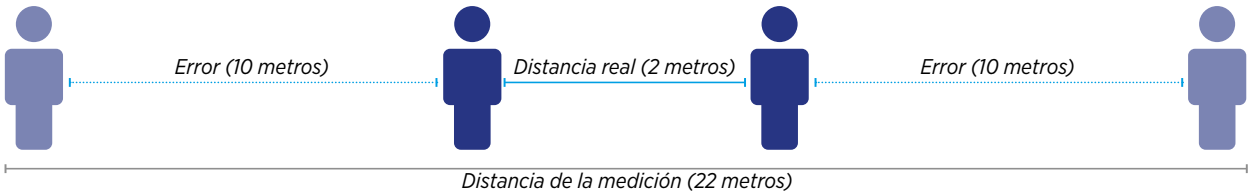
Bluetooth



GPS (Outdoors)



Wifi



El método más popular es el de usar la fuerza de la señal *Bluetooth* para inferir la distancia entre los dispositivos. En este caso, el rastreo digital de interacciones utiliza la BLE de los teléfonos móviles para detectar otros móviles y medir la distancia a la que se encuentran. Esta tecnología implica un menor uso en comparación con el *bluetooth* que normalmente se utiliza para conectar un móvil a otros equipos, como los auriculares. Si un teléfono se encuentra cerca de otro por un tiempo determinado, los móviles implicados intercambian un "identificador efímero", es decir, un código aleatorio que sirve para identificar el dispositivo y que se guarda en el teléfono. Si bien la distancia y el tiempo son configurables, las soluciones que se han observado suelen estar calibradas para identificar un contacto cuando su móvil está a menos de dos metros de

otro móvil que tenga instalada la *app*, durante más de 15 minutos. Si uno de los usuarios reporte ser positivo en la app, su teléfono manda una alerta a los códigos aletarios que ha recibido para notificarles del caso.

Este es un sistema que complementa el rastreo manual y que permite, asimismo, enviar alertas a personas de las que la persona que ha dado positivo no tiene constancia (compañeros de viaje en el transporte público, por ejemplo). El rastreo digital constituye así una medida de alerta temprana ya que la notificación de la exposición se recibe antes de que aparezcan los síntomas; si un usuario estuviese en fase asintomática o presintomática (40-60% de los casos) podría tomar medidas cuanto antes, evitándose de esta manera nuevos contagios.

La principal limitante de esta solución radica en que los sistemas operativos de los *smartphones* cuentan con medidas para proteger el consumo de la batería y la privacidad de los usuarios. Estas medidas (especialmente en el sistema iOS) hacen que las aplicaciones puedan no funcionar correctamente mientras están en segundo plano (*background*), lo que obliga a los usuarios a tener la aplicación en constante funcionamiento o a abrirla periódicamente para reiniciar el proceso.

Ante estas dificultades los dueños de los sistemas operativos más populares (Apple y Google) crearon una solución conjunta llamada *Exposure Notification System* o Sistema de Notificación de Exposición.

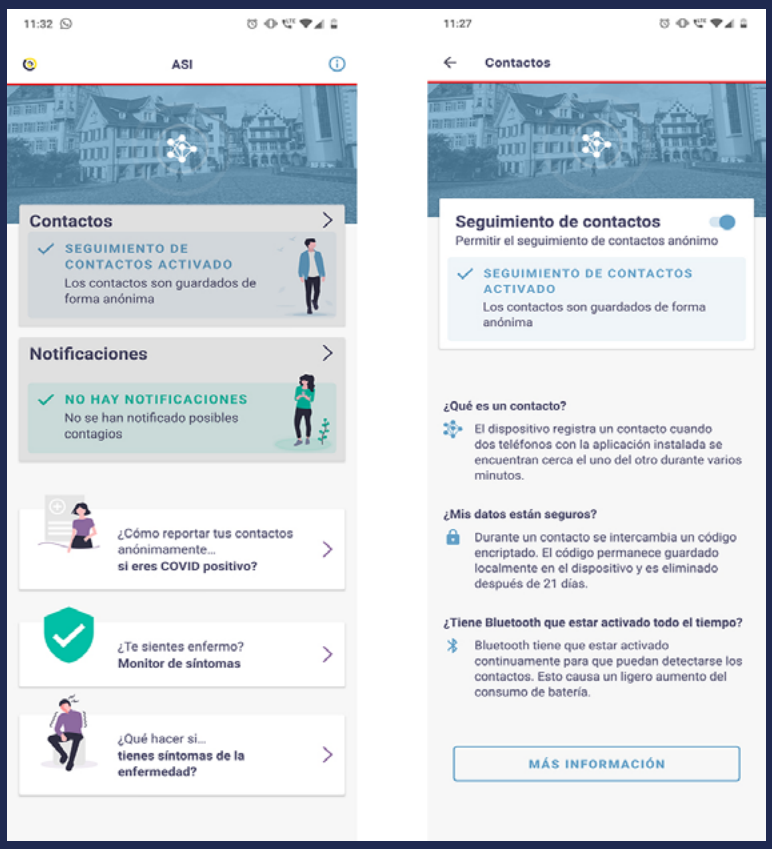
Apple/Google ENS (Exposure Notification System)

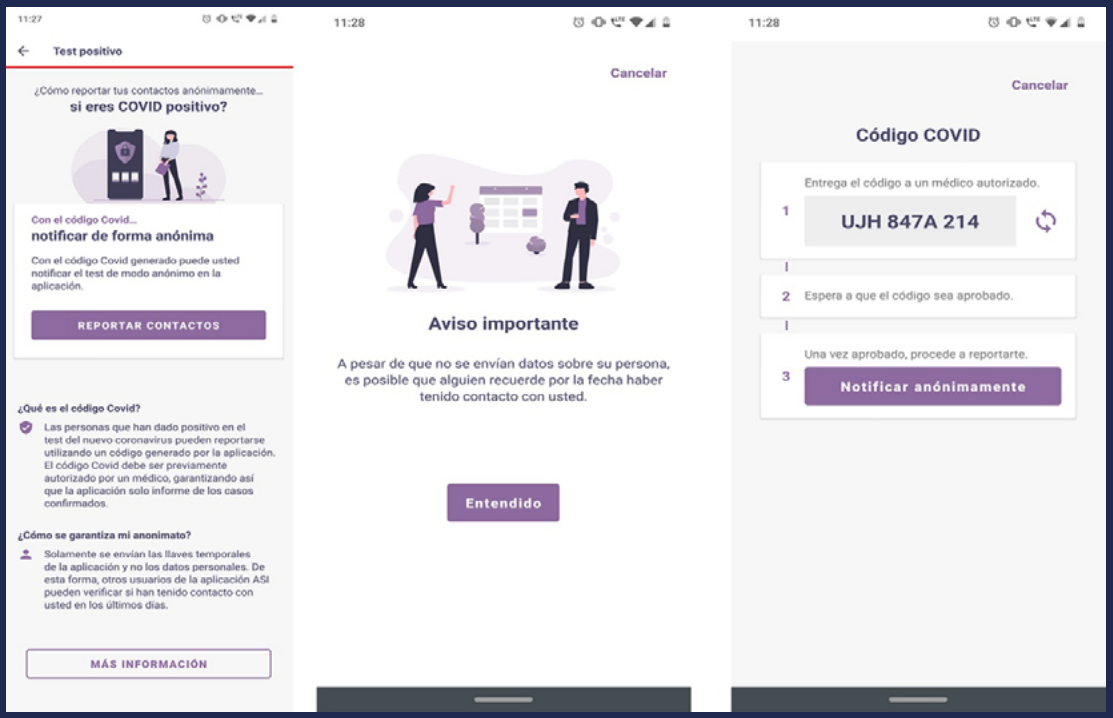
Esta nueva capacidad del sistema operativo permite registrar las interacciones con otros teléfonos que tengan la app en modo *background* y con mayor precisión. La información se maneja a nivel de sistema operativo y está disponible para aplicaciones autorizadas que deben ser aprobadas por Apple/Google y tener el aval de entidades gubernamentales, por lo que no son viables para programas privados.

Esta es una solución diseñada para proteger la privacidad y no permite ver la información de otros contactos. Para ello guarda toda la información de los contactos en el teléfono inteligente por un periodo de tiempo determinado, normalmente 14 días, y la anonimiza usando identificadores temporales generados por claves rotatorias.

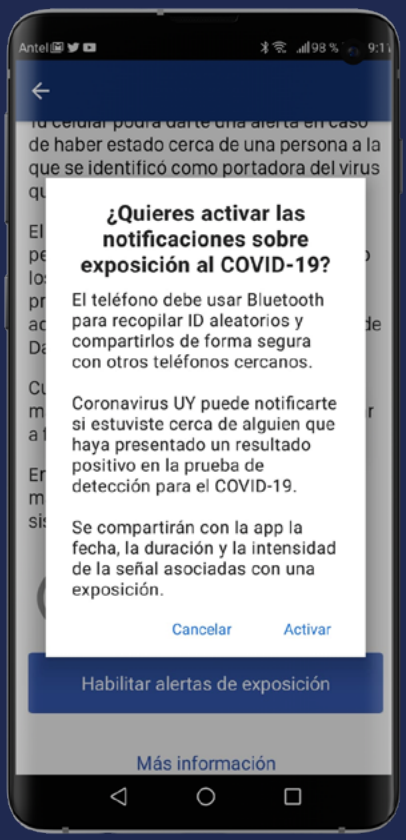
Cuando los organismos correspondientes identifican a un contagiado le pedirán al usuario/a sus claves rotatorias de los últimos 14 días. Estas claves son subidas a un servidor que las descarga en la aplicación móvil instalada en los teléfonos del resto de los usuarios. La aplicación usa un algoritmo para recrear los identificadores temporales y comprobar si se encuentran entre los contactos registrados en el periodo relevante. En caso de encontrar un contacto con este identificador, se envía una notificación al usuario/a de la aplicación con los pasos que debe seguir según las recomendaciones de cada de uno de los países o Estados. Este tipo de aplicaciones han sido lanzadas y están siendo utilizadas actualmente en Ecuador, Uruguay (Recuadros 1 y 2), y Brasil.

Recuadro 1: Ejemplos del sistema de rastreo digital implementado en Ecuador





Recuadro 2: Ejemplos de sistema de rastreo digital implementado en Uruguay



La *Exposure Notificacion Express*[5], una nueva implementación del ENS, permite a los gobiernos acceder a estos servicios sin desarrollar una aplicación propia. La compañía Apple integró estas habilidades en el sistema operativo y Google creó una aplicación genérica que los usuarios pueden usar para registrarse en los programas de sus gobiernos. Esto forma parte de un esfuerzo conjunto para reducir los costos y tiempos de implementación, y favorecer que los usuarios instalen la aplicación. Sin embargo, si bien realiza las tareas básicas de ENS, se pierden posibilidades de comunicación, cambio de comportamiento e integración que una aplicación completa puede ofrecer[6].

5 Para más información se pueden consultar las guías proporcionadas por Apple y Google, la información publicada por el consorcio DP3T que desarrolló el protocolo base, o el código de las aplicaciones ya existentes, que todos los países han publicado en repositorios abiertos.

6 Aunque se están desarrollando alternativas como interfaces web para solventar estos temas.

Consideraciones para la adopción de tecnologías de rastreo de contactos

Antes de implementar un sistema digital de rastreo de contactos hay que plantearse una serie de preguntas que guíen la decisión. Las más relevantes a continuación.

¿Modelos centralizados o descentralizados?

A grandes rasgos, existen dos modelos o enfoques para rastrear interacciones a través de *apps:* el centralizado y el descentralizado[7]. Las **principales diferencias** entre ambos son:

a La cantidad y el tipo de información a la que tienen acceso las autoridades sanitarias.

b Las implicaciones de su uso para la protección de datos.

c Su capacidad para interoperar con otros sistemas.

En el modelo centralizado, al descargar la *app*, el usuario proporciona su número de teléfono y este dato, así como todas sus interacciones, son recogidos en una base de datos centralizada. Si el usuario es diagnosticado como positivo por COVID-19, las autoridades sanitarias pueden acceder inmediatamente a sus datos y a los teléfonos móviles de sus interacciones.

Al recoger los datos personales el modelo centralizado es más vulnerable a un posible *hackeo* de información sensible (existe un servidor con información médica sensible que podría ser atacado). Esto ha hecho que diferentes autoridades de protección de datos, como la noruega o la italiana, hayan declarado la ilegalidad del modelo centralizado al no cumplir con el principio de protección de datos.

En el modelo descentralizado, en cambio, el usuario no necesita proporcionar ningún tipo de información personal (ni el nombre, ni el número de teléfono, ni el estado de salud, ni ningún otro tipo de dato personal) y las autoridades sanitarias no tienen ningún acceso al historial de interacciones de los usuarios. Si un usuario/a es diagnosticado positivo por COVID-19, se le proporciona un código de autenticación que el mismo usuario debe registrar en su teléfono. Los

7 Si bien algunos países como Francia o Singapur hablan de modo híbrido este es, en realidad, centralizado para efectos de esta discusión.

teléfonos que contienen la aplicación pueden bajar las listas de aquellos códigos que dieron positivos, ver si coinciden con los códigos guardados en cada teléfono y dar la alerta si fuera el caso. De esta manera no es necesario que un teléfono guarde información que sirva para identificar a un contacto.

Finalmente, sólo las *apps* descentralizadas pueden acceder a la Interfaz de Programación de Aplicaciones (API por sus siglas en inglés) de Google y Apple, lo que permite la activación permanente del BLE y el funcionamiento de la *app* sin que ello implique erosión de la batería. En términos de interoperabilidad, contar con tecnología que sea conectable y especificaciones que puedan traducirse a un único estándar, es algo que facilita la movilidad entre países de forma segura, al permitir que las *apps* recojan interacciones incluso en otros países. Un ejemplo ilustrativo es la experiencia de Gran Bretaña, que luego un resultado negativo en el modelo centralizado adoptó el modelo descentralizado basado en la tecnología de Google y Apple.

Otra ventaja es que los sistemas operativos sobre los que funcionan estas *apps* son propiedad de Google y Apple, las dos compañías que controlan las tiendas de *apps* y los sistemas operativos de la mayoría de los teléfonos móviles del mundo. El rol de estos actores se centra en permitir el acceso de las *apps* al BLE, y no acceden ni pueden acceder a la información contenida en la *app* ni a ningún dato relativo al estado de salud de los usuarios/as, o a las alertas que hayan podido recibir.

¿Realmente funcionan?

Estas aplicaciones se basan en una idea innovadora que ha demostrado tener mucho potencial en modelos de simulación. En los países en los que ya llevan semanas funcionando, como Alemania, Ecuador o Uruguay, existe constancia del envío de alertas a usuarios sobre la existencia de un riesgo de contagio. Sin embargo, aún es pronto para contar con datos sobre su impacto real o para saber su contribución específica sobre la capacidad de respuesta a la COVID-19 por parte de los países. Los ejemplos de aplicaciones previas como las que se utilizaron en Israel o Singapur no se pueden considerar como evidencia a favor o en contra debido a que el modelo que utilizaron tiene serias debilidades (la falta de interoperabilidad entre sistemas operativos y la limitación al uso de BLE por ejemplo) y funcionan de forma muy diferente a las *apps* descentralizadas.

¿Qué necesita un país para desarrollar una app de rastreo de interacciones?

Muchos de los países que utilizan *apps* descentralizadas han dispuesto el código de la *app* en repositorios libres para que los sistemas puedan ser utilizados y adaptados a cada país que lo necesite. Actualmente existen diferentes modelos que pueden reutilizarse y adaptarse, por ejemplo, en cuanto a la distancia y tiempo de contacto que se considera un riesgo y la interfaz de usuario y el sistema de generación de autorizaciones por parte del sistema de salud.

No obstante, los países interesados en desarrollar *apps* descentralizadas deberán tener en consideración una serie de requisitos técnicos y de gobernanza:

Aspectos técnicos:

a) Un porcentaje significativo de población con teléfonos móviles inteligentes de generaciones recientes.

b) Un porcentaje significativo de población que se descargue la *app*. Aunque los estudios iniciales hablaban de la necesidad de un índice de adopción superior al 60%, análisis recientes concluyen que la *app* es útil incluso con niveles de adopción mucho menores.

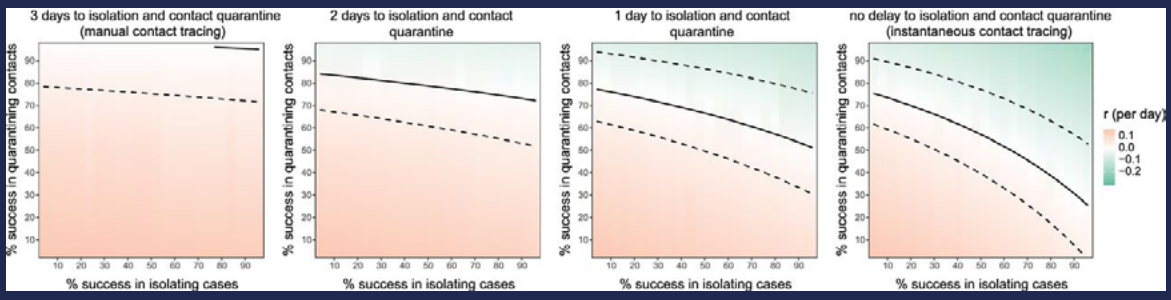
Recuadro 3: Relación entre efectividad y adopción de la aplicación

Una simulación del equipo de Oxford que planteó la idea del 60% da una visión menos categórica sobre cómo funcionaría una aplicación de rastreo de interacciones. En esta simulación se hacen varios supuestos acerca de las características epidemiológicas del virus y se muestran los "efectos en r" de diferentes combinaciones de dos variables:

Eje horizontal: Porcentaje de casos sintomáticos que se aíslan inmediatamente, y

Eje vertical: Porcentaje de contactos que se aíslan con diferentes números de días de retraso.

Las áreas verdes en los gráficos muestran los casos en los que se logra un crecimiento de r negativo, las áreas en rojo muestran un crecimiento positivo.



Fuente: Ferretti L, Wymant C, Kendall M, Zhao L, Nurtay A, Abeler-Dörner L, Parker M, Bonsall D, Fraser C. Quantifying SARS-CoV-2 transmission suggests epidemic control with digital contact tracing. Science. 2020 May 8;368(6491):eabb6936. doi: 10.1126/science.abb6936. Epub 2020 Mar 31. PMID: 32234805; PMCID: PMC7164555.

En el caso de tres días de retraso en aislar a contactos no se muestra ningún escenario de reducción de r. Sin embargo, en el caso de trazabilidad instantánea de contactos se muestra un área verde para varias combinaciones de los parámetros utilizados.

Existen varios otros ejercicios que tratan de simular este tipo de efectos, los resultados por supuesto dependen de los varios supuestos detrás de los parámetros pero el punto al final del día es que incluso a bajos niveles de adopción parece haber un valor agregado del uso de estas aplicaciones, lo que se debe considerar es si el valor agregado de una aplicación para un nivel dado de adopción justifica la inversión (no solo financiera sino en RRHH) en una solución de este tipo.

c) Capacidad de testeo y cuarentena. Es deseable que, en el momento de recibir una alerta, los contactos de una persona que ha dado positivo tengan acceso inmediato a una prueba PCR o a lugares donde cumplir una cuarentena preventiva. No obstante, incluso ante la ausencia de capacidad de testeo, es preferible que las personas que han estado en situaciones de riesgo sean notificadas y puedan tomar las medidas pertinentes.

d) Existencia de *call centers* y/o centros para la emisión de autorizaciones. Las buenas prácticas indican que las *apps* no deben permitir que los usuarios se autodiagnostiquen

como contagiados, ya que es algo que se ha de hacer en función de un código emitido por las autoridades sanitarias. Es necesario contar con los mecanismos necesarios para que desde la atención primaria o desde un centro específico se puedan proporcionar estos códigos a las personas diagnosticadas como positivos por COVID-19.

Aspectos de gobernanza:

e) Un Ministerio de Salud con un papel rector de la aplicación que utilice la API de Google y Apple. Esto requiere que el Ministerio se registre en el programa de adopción temprana de estas empresas y solicite los derechos, un proceso que puede ser largo y muy técnico. El Ministerio de Sanidad deberá, además, ser el titular del servidor de identificadores efímeros que permite el sistema de alertas.

f) Una mesa de coordinación técnica interministerial. Las *apps* de rastreo digital solo pueden ser promovidas por una autoridad sanitaria. No obstante, su éxito depende de la coordinación entre diferentes actores, que deberán trabajar de forma conjunta y coordinada para desarrollar la *app*.

g) Un equipo técnico de tecnologías de la información. Aunque las especificaciones de la *app* se encuentran en repositorios abiertos, cada país debe adaptar el sistema, para lo que será necesario un apoyo técnico especializado.

h) Apoyo del equipo de epidemiología. El seguimiento o rastreo de contactos es una de las funciones más importantes de la vigilancia epidemiológica y, como ya se ha expuesto, consiste en la identificación de todos los contactos estrechos de un caso de COVID-19 para poder realizarles el seguimiento de su estado de salud. Su apoyo es esencial en la digitalización de este proceso.

i) Apoyo del equipo de comunicación. El éxito de las *apps* depende en gran medida de que la población entienda su funcionamiento y confíe en que su uso es seguro. Para conseguir una adopción generalizada se deberán programar una campaña de comunicación amplia y accesible, y una política de transparencia activa.

Además de estos elementos esenciales, hay otros que, si bien no son imprescindibles, son deseables:

a) Disponer de un marco legal enmarcado en el uso, seguridad y privacidad de los daos que tendrá la *app*.

b) Contar con el aval favorable de la autoridad de protección de datos con anterioridad al despliegue de la *app* y que ésta sea parte de la mesa de coordinación técnica.

c) Desarrollar unos términos de aceptación incluyendo el consentimiento informado para asegurar que la *app* es voluntaria, que su uso no puede implicar ningún privilegio, y que establezca los derechos y deberes de los usuarios.

d) Adaptar la *app* para su uso por parte de personas con algún tipo de discapacidad.

e) Contar con la infraestructura necesaria y los subsidios para facilitar el aislamiento de las personas alertadas, para que no ponga en riesgo a su familia ni círculo cercano de contactos.

f) Adoptar acuerdos para que el uso de la app no consuma datos (*data free*) facilitando su uso por parte de personas que no disponen de planes ilimitados de uso de datos.

g) Contar con infraestructura tecnológica (que incluya normas y estándares que deben cumplir los data centers) para los servidores donde se suben los códigos, así como con personal para mantener y proteger estos servidores. Si los servidores no están disponibles por problemas técnicos se anula el efecto de la *app*.

h) Llegar a acuerdos con las Comisiones Nacionales de Bioética cando estas existen o asegurar la incorporación de aspectos morales, jurídicos y sociales relacionados con la investigación, la experimentación y la aplicación de nuevas tecnologías en el campo de las ciencias de la vida y la salud.

¿Por qué estas aplicaciones pueden ayudar de manera individual y colectiva?

Las personas que utilizan la *app* contribuyen significativamente en la respuesta a la pandemia ya que al ser alertadas de su posible riesgo y tomar medidas, protegen al resto de la población, incluyendo a aquellos que no la utilizan.

Riesgos y salvaguardias

a) Riesgo general de exclusión

Las *apps* de rastreo de interacciones sólo podrán ser utilizadas por personas mayores de edad que dispongan de teléfonos móviles inteligentes relativamente recientes (menos de 5 años)[8]. Esto implica la exclusión de una parte importante de la población debido a la brecha digital y a consideraciones socio-económicas. No obstante, las *apps* son una medida que complementa otras como el rastreo manual, las mascarillas, la distancia social, etc., y no proporcionan ningún privilegio vinculado a su uso, razón por la que se considera que esa exclusión no genera efectos negativos.

Para mitigar que otros colectivos puedan verse excluidos por motivos de accesibilidad, las *apps* deberán contar con interfaces adaptadas y facilidades para que las personas con discapacidad puedan utilizarlas sin problemas. Adicionalmente, en la

8 También existen algunos modelos específicos que, sin ser antiguos, no funcionan con la tecnología de Google y Apple, como el Huawei Mate 30, el Huawei P40 y el Honor 30. https://www.xda-developers.com/huawei-hms-core-contact-shield-api-covid-19-contact-tracing/

fase de pilotaje se deberán tener en cuenta diferentes perfiles socio-económicos para adaptar el lenguaje y los procesos a diferentes necesidades, facilitando su comprensión por parte de colectivos menos familiarizados con la tecnología.

Finalmente, la *app* solo deberá requerir de un plan de datos o acceso a Wi-Fi en el momento en que se introducen los códigos de verificación. La operativa cotidiana de la *app*, idealmente, no consume datos.

b) Riesgo de exclusión de mayores y menores

Jóvenes y mayores son dos importantes grupos en situación de vulnerabilidad cuando se trata del potencial uso de las *apps.* En el caso de los jóvenes, porque su uso solo está permitido para los mayores de edad; en lo que a los mayores se refiere, por estar menos familiarizados con la tecnología. En el contexto de la presente pandemia, esto no se considera un problema grave, en primera instancia por el efecto de protección de los menores; y en segunda instancia porque, en realidad, aunque los mayores son uno de los grupos de riesgo, los vectores de contagio se encuentran entre los más jóvenes y los adultos que, por motivos sociales o laborales, tienen más interacciones y con ellas más probabilidades de contagio. Así pues, en la pandemia de COVID-19 son los usuarios de teléfonos menos actualizados quienes menos se van a beneficiar de la existencia de una *app* de rastreo de interacciones. Países como Singapur han intentado crear dispositivos portátiles o *wearables* para resolver este problema.

c) Riesgo de falsos positivos

Por diferentes motivos, es posible que la alerta que reciba un usuario no se traduzca en un contagio efectivo. Esto puede deberse a varios motivos: presencia de anticuerpos, uso de mascarilla y/o distancia social, o error en la calibración del riesgo por parte del BLE, entre otros. En el contexto de la COVID-19, no obstante, los falsos positivos no se consideran un problema importante: cualquier protección es poca ante la enfermedad, y un falso positivo es una persona más que tomará precauciones, lo que, a la larga, es algo beneficioso.

d) Fatiga de los usuarios.

También es importante tener en mente la fatiga de los usuarios, es decir, si una persona es notificada constantemente de que estuvo en contacto con un posible positivo, puede perder confianza en el sistema y decidir no participar.

e) Riesgo de invasión de la privacidad

Las *apps* descentralizadas que utilizan BLE no recogen ni siguen la localización de los usuarios (en Google/Apple, está prohibido por diseño). Como se explicó con anterioridad, lo único que se registra son encuentros anónimos entre usuarios, y solo se hace en los dispositivos de los usuarios, La información no se comunica a ningún servidor central. Ni siquiera el usuario podría utilizar la información generada para conocer su historial de interacciones, ya que estas solo registran un identificador efímero aleatorio y una franja temporal. La privacidad es el valor fundamental que las *apps* descentralizadas buscan salvaguardar, por lo que han sido diseñadas siguiendo las

directrices de la Privacidad desde el Diseño. Todos los datos generados son anónimos (identificadores efímeros), no son almacenados y se eliminan en un período determinado (normalmente 14 días), o cuando la *app* es desinstalada, previniendo así posibles hackeos o filtraciones. Igualmente, cuando ya no se producen contagios, la *app* deja de tener sentido y se suspende automáticamente al no recibir códigos que generen alertas.

f) Riesgo de mal uso por parte de los usuarios

Para minimizar el riesgo de mal uso algunos gobiernos han establecido que los usuarios no puedan lanzar alertas si no reciben un código generado por el sistema de salud tras un positivo verificado. No es posible pues, que los usuarios generen alertas de forma autónoma.

g) Riesgo de ataque malintencionado (ciberseguridad)

Uno de los ataques que se ha descrito para estas *apps* sería un ataque a los sistemas *Bluetooth* utilizando *sniffers*[9], un escenario poco probable ya que requeriría altos costos para llevarlo a cabo (instalación física de *snfiffers* en una superficie considerable) y beneficios bajos (trazabilidad de los usuarios que hubieran pasado por esa superficie, pero no necesariamente re-identificación).

h) Riesgo de acceso a los datos por parte de terceros

El uso de *apps* descentralizadas de rastreo de interacciones no genera riesgos adicionales de acceso a los datos por parte de Google y Apple. Estos proveedores de los sistemas operativos de la mayoría de los teléfonos inteligentes del mundo tienen acceso al uso de sensores. Si Google o Apple quisieran acceder a datos de los usuarios no necesitarían estas *apps*, puesto que ya controlan el sistema operativo y los sensores. Aunque no conviene descuidar este riesgo, es algo que afecta a temas más generales sobre privacidad y no solo a este caso particular de rastreo de contactos.

Al incorporar estas tecnologías los los gobiernos deben gestionar sus propios servidores para subir y distribuir las claves rotatorias de las personas contagiadas. La información que estos servidores comparten, es decir las claves de positivos, fueron diseñadas para ser distribuidas y no revelan información con respecto a los usuarios/as y sus comportamientos.

i) Riesgo de que no funcionen las apps

Este riesgo puede tener dos causas. La primera es que por alguna razón la tecnología no funcione en los países en los que se implementan las soluciones, ya sea por falta de precisión en BLE o por el tipo de teléfonos que se utilizan en un país. El segundo riesgo es que, aunque la tecnología funcione, no sea suficiente para tener un impacto en la tasa de infección, debido, por ejemplo, a que el tiempo o la distancia necesarias para el contagio son menores o mayores de las que mide la aplicación, respectivamente.

9 Herramientas digitales dirigidas a interceptar flujos de datos en tiempo real para robar información a través de la obtención de paquetes de redes de tráfico de datos.

Algunas lecciones ya aprendidas

Son ya muchos los países que han implementado *apps* de rastreo de interacciones. Entre los que han optado por modelos centralizados, sabemos que la **tasa de adopción** ha sido baja (Francia, Singapur) y que no se ha apreciado una contribución sustancial de las *apps* a la disminución de los contagios. En otros casos, como el de Noruega, las autoridades de **protección de datos** han declarado ilegal la *app* desarrollada por su uso de un servidor centralizado. En el caso británico, la *app* centralizada desarrollada inicialmente ha sido ya descartada por una combinación de los problemas descritos (baja adopción y dudas sobre su legalidad), a los que se ha sumado la imposibilidad de que los modelos centralizados accedan a la tecnología de ENS, lo que resulta en la inhabilitación del BLE cuando la *app* no está activa y en un gran consumo de batería. Según la experiencia internacional, solo las *apps* descentralizadas son viables.

Entre los países que han adoptado *apps* descentralizadas la experiencia es también, distinta y aún es pronto para sacar conclusiones puesto que las *apps* descentralizadas compatibles con la API de Google y Apple se empezaron a lanzar dos meses antes de la publicación de esta nota. Se debe subrayar el **esfuerzo comunicativo** realizado algunos países, como Alemania, el país que más éxito ha obtenido, de momento, en tasas de adopción de la *app*. La misma canciller Angela Merkel se implicó en ese esfuerzo, animando a la población a utilizar la *app* y presentándola en un acto al más alto nivel, con presencia ministerial.

En términos generales el éxito de estas *apps* se basa en cuatro elementos: comunicación, coordinación, privacidad e integración con la API de Google y Apple.

Indicadores de éxito

Las *apps* de rastreo de interacciones están aún en una fase muy incipiente. Su implementación real es muy reciente y todavía no se cuenta con datos de evaluación sólidos. No obstante, los esfuerzos para valorar la utilidad e impacto de estas *apps* en la lucha contra la pandemia se centran en:

a) Evaluar la experiencia de usuario realizando estudios y seguimiento con subgrupos de usuarios. En este caso, los indicadores de éxito son la descarga y uso activo de la *app*, y las acciones preventivas tomadas tras la comunicación de alerta medidas a partir de las interacciones con los servicios de atención médica.

b) Evaluar la integración operativa. En este caso, los indicadores de éxito son la emisión de códigos de autorización y la incorporación efectiva del elemento *app* en los protocolos de atención a los usuarios.

c) Evaluar el funcionamiento del BLE en función de las alertas generadas. Los indicadores de éxito serán el número de alerta generadas y su relación con los datos obtenidos por los procesos de rastreo manual.

En última instancia, al formar parte de un ecosistema de combate contra la pandemia, el indicador de éxito definitivo será la posibilidad de romper las cadenas de contagio sin recurrir al confinamiento general.

Recomendaciones principales

Implementar aplicaciones de rastreo de interacciones es, técnicamente, relativamente sencillo, pero reviste complejidad desde el punto de vista de la integración operativa con los flujos de atención sanitaria.

En general se recomienda,

1. ***Utilizar sistemas descentralizados y basados en BLE.***
La experiencia internacional hasta el momento muestra que los sistemas más viables y exitosos son las aplicaciones móviles que utilizan BLE y gestionan los datos de forma descentralizada, respetando y protegiendo la privacidad de las personas.

2. ***Utilizar soluciones publicadas por otros países.***
La mayoría de los países que ya han desplegado estas soluciones han publicado el código de sus *apps*, por lo que los países que deseen adoptarlas solo deberán adaptarlas a sus peculiaridades. En algunos casos los países han compartido también detalles sobre sus decisiones de integración operativa, pero este paso dependerá de las características de los sistemas de salud locales y de sus diferentes niveles de digitalización.

3. ***Preparar una buena integración operativa liderada desde el gobierno y los responsables de Sanidad.***
El éxito de estas aplicaciones no depende solo de temas técnicos, sino de la integración de las alertas móviles en un sistema de atención y seguimiento de salud. Disponer de un flujo de trabajo integrado y bien coordinado es esencial para que las notificaciones sean útiles en el combate contra la COVID-19.

4. ***Crear un buen equipo técnico multidisciplinar y transversal.***
La implementación efectiva de las *apps* de rastreo requiere una coordinación entre diferentes ministerios y equipos, tanto técnicos como médicos, así como la realización de campañas de sensibilización amplias y certeras.

5. ***Realizar un piloto previo a la implementación general.***
Debido a las complejidades técnicas y de integración operativa, los países que quieran implementar estas aplicaciones tendrán más posibilidades de éxito si planifican un piloto previo, breve, que permita poner a prueba temas de experiencia de usuario, funcionamiento técnico e integración con el sistema de salud, así como la emisión de códigos de alerta.

6. ***Preparar una campaña de comunicación.***
El éxito del sistema depende de su adopción por parte de la ciudadanía. Por lo tanto, es imprescindible que reciba una información transparente y orientada a generar confianza e incentivos para la descarga y uso de la *app*. La campaña debe poner especial esfuerzo en llegar a grupos tradicionalmente excluidos.

* Las referencias citadas en esta nota pueden ser consultadas aquí o por solicitud a los autores.