Escudo digital

Tecnología al servicio de la ciudadanía durante emergencias sanitarias

---

Jorge Juan Ramos Garnero
Julio 2021

1. Introducción

Durante la pandemia global que comenzó a finales de 2019, hemos visto cómo gobiernos de todo el mundo, y por lo tanto de toda filiación política, han enfrentado en problema del rastreo de contactos de diferentes formas.

El rastreo de contactos es una herramienta eficaz para evitar eventos de propagación en epidemias y pandemias, tal y como se demostró durante la epidemia de ébola en Liberia en 2014-2015.[1]

Es evidente que la primera línea de actuación en este aspecto es (y debe ser) la mas elemental de todas: el rastreo manual realizado por personas que preguntan a otras personas que han resultado positivas en un test, cuáles han sido sus contactos de riesgo durante los últimos días. De este modo, se pueden identificar posibilidades de contagio para tratarlas y aislarlas si fuera oportuno, evitando así eventos de super propagación.

Siendo el rastreo de contactos manual eficaz y necesario, se pueden dar diversos factores por los cuales éste pierda su eficacia: falta de personal, falta de medios o la imposibilidad de algunos pacientes para recordar algunos de sus contactos de riesgo.
Independientemente de los criterios médico-científicos que definan un contacto de riesgo, es probable que un paciente no pueda recordar todos y cada uno de ellos.

En enfermedades que se transmiten principalmente por el aire, como es el caso del *COVID-19*[2], un contacto de riesgo puede llegar a definirse mas allá de las reglas básicas 2 metros/15 minutos que se definió durante 2020. Esto amplía exponencialmente por lo tanto el número de posibles contactos de riesgo que una persona infectada puede tener, siendo éste inversamente proporcional a la capacidad de la persona infectada para recordarlo todos.

Es en este punto en el que la tecnología digital, a la que la mayoría de la población puede acceder de manera regular justo en este momento del S.XXI, es de utilidad demostrada[3] junto con el resto de medidas clásicas para eventos mundiales de este tipo.

1.1 Contenido de este informe

En este informe se va a analizar, en un lenguaje no técnico, la necesidad de crear una red preventiva digital ante la amenaza de una emergencia sanitaria. Hay que comprender el concepto *escudo digital* como una entidad no monolítica, capaz de amoldarse a la gravedad de la amenaza y construida sobre siete pilares básicos e inamovibles:

- **Privacidad primero (privacy first)**: ninguna de las tecnologías que conformen un escudo digital utilizará datos personales para cualquiera de sus funciones. Sin excepciones. Se entienden como datos personales cualquier tipo de información, en cualquier formato, capaz de identificar unívocamente a un ciudadano, por ejemplo: posición *GPS*, números de teléfono, números *IMEI* o cualquier otro identificador único de hardware, direcciones email, direcciones *IP*, etc.

- **Open Source**: Todo el código fuente que constituya el escudo digital, o cualquiera de sus partes integrantes, deberá ser publicado para el análisis y auditoría por profesionales independientes.

---

[1] Swanson, Krista C et al. “Contact tracing performance during the Ebola epidemic in Liberia, 2014-2015.” PLoS neglected tropical diseases vol. 12,9 e0006762. 12 Sep. 2018, doi:10.1371/journal.pntd.0006762. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6152989/

[2] Lidia Morawska, Joseph Allen et al. A paradigm shift to combat indoor respiratory infection. SCIENCE14 MAY 2021 : 689-691 https://science.sciencemag.org/content/372/6543/689

[3] Wymant, C., Ferretti, L., Tsallis, D. et al. The epidemiological impact of the NHS COVID-19 Aplicación. Nature (2021). https://doi.org/10.1038/s41586-021-03606-z

- **Modularidad**: un escudo digital eficaz es aquel que puede adaptar su capacidad operativa en función del tamaño de la amenaza sanitaria, habiendo sido previamente evaluada dicha amenaza por equipos competentes en la materia. Su arquitectura debe ser capaz de activar o desactivar funciones operativas a demanda y en el menor tiempo posible: horas y no días.

- **Transversalidad**: el escudo digital sólo será eficaz al 100% si es capaz de llegar a toda la población. Debido a factores que escapan al alcance de este informe, como la llamada *brecha digital*[4], alcanzar esta cota es virtualmente improbable. Sabiendo esto, todas las técnicas que constituyan un escudo digital deben encontrar el equilibrio entre capacidad operativa técnica y penetración social. En otras palabras: se deben usar tecnologías que estén disponibles para el mayor porcentaje de población posible, huyendo de complejidades o condicionamientos por capacidad económica, además de proveer una solución "analógica" o tradicional para cada uno de los elementos que conforma el escudo digital.

- **Desmantelamiento elegante (graceful dismantling)**: Un escudo digital completo será aquel que sea capaz de auto desmantelarse cuando ya no sea necesario. Sin intervención de terceros: si la ciudadanía deja de usarlo, se volverá inservible y toda la información y relaciones que contenga desaparecerá, debido a su carácter volátil. Las razones por las que se deje de usar un *escudo digital* deberán atender sólo y exclusivamente a razones médicas y/o epidemiológicas. Y cuando esto ocurra, el *escudo digital* desaparecerá por si mismo, no dejando rastro alguno en ninguno de los actores.

- **Descentralización**: No existirá un servidor o cualquier tipo de procesador informático central que acapare toda o parte de la información de todos o alguno de los módulos del *escudo digital* con fines computacionales. Todo el procesamiento de datos productivo deberá ser descentralizado y por lo tanto realizarse en los terminales móviles.

- **Accesibilidad**: Las soluciones digitales irán encaminadas hacia la mayor parte de la población posible, y por lo tanto no se pueden obviar los grupos de población con discapacidades físicas. El *escudo digital* ha de facilitar su uso a estas personas mediante un diseño y experiencia de uso adaptadas y comprometidas con discapacidades físicas importantes, tales como ceguera o sordera total o parcial, *Parkinson* o cualquier otro tipo de enfermedad o condición que imposibilite el uso estándar de cada una de las soluciones que conforman el escudo digital.

No existirá escudo digital si se incumple uno solo de estos pilares básicos. Es importante comprender que es posible una aplicación práctica de la tecnología de forma responsable y respetuosa con los ciudadanos, a la vez que es eficaz en el cometido para el que se va a diseñar.

2. Escudo digital

Un *escudo digital* es el resultado de la inclusión y utilización de diferentes técnicas y herramientas tecnológicas que, de forma descentralizada, anónima y continua, colaboran entre sí con el único fin de monitorizar la situación epidemiológica de un territorio y así mitigar sus efectos en la medida de lo posible.

Una de las formas de tecnología más populares en los últimos años es la tecnología móvil. Actualmente un gran porcentaje de la sociedad en Europa, América y Asia junto con Australia y Nueva Zelanda tiene acceso a tecnologías móviles a diario.
Según un informe publicado por *CISCO*[5], en 2023 un 70% de la población mundial dispondrá de un terminal móvil. En el caso de Europa, el informe estima un 88% para la Europa Occidental y un 81% para la Europa Central y Oriental.
Del mismo modo, sus gobiernos centrales y locales disponen de capacidad para desarrollar soluciones tecnológicas que aprovechen las características y den soporte a dicha tecnología móvil.

---

[4] Brecha digital. https://es.wikipedia.org/wiki/Brecha_digital

[5] Cisco Annual Internet Report (2018–2023) White Paper https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

Con estos datos y perspectiva, parece factible contar con una red digital que proteja a la población ante eventos de este tipo el 100% del tiempo, ofreciendo una protección no sólo en materia de salud sino también propiciando una pronta recuperación económica.

Llegados a este punto es muy importante recalcar que un *escudo digital* no es sólo un parque de aplicaciones móviles con mayor o menor impacto. Un *escudo digital* también comprende labores de comunicación e informativas, así como el apoyo institucional y la formación continua a la población, de tal modo que la confianza suponga el menor problema posible. Del mismo modo, expertos en otras soluciones de hardware y tecnología aplicada deberán pronunciarse para cubrir el mayor espectro posible, consiguiendo así un *escudo digital* lo más completo y eficaz posible.

Un estudio acerca de la calidad y adopción de las aplicaciones móviles contra la *COVID-19* en Europa[6] propone una serie de mejoras en dichas aplicaciones que, junto con otras propuestas, podrían conformar un escudo digital completo desde el punto de vista de la movilidad que comprenda:

- Soluciones preventivas
  - Rastreo de contactos
  - Etiquetado de lugares (*venue tagging*)
  - Gestión integral de tests
  - Herramientas de auto diagnóstico
  - Protocolo estándar de medición de CO_2

- Soluciones informativas
  - Monitores epidemiológicos en tiempo real
  - Canales de información epidemiológica
  - Canales de comunicación institucional

- Soluciones facilitadoras
  - Sistemas de educación a distancia
  - Sistemas de consulta médica a distancia
  - Sistemas de solicitud y distribución de bienes de primera necesidad
  - Atención psicológica

Se analizarán una a una estas propuestas, aportando una visión técnica clara acerca de alternativas de implementación y proponiendo soluciones prácticas apoyadas en el trabajo que otros han venido haciendo durante todo el año 2020 y finales de 2019.

ESCUDO DIGITAL

PREVENCIÓN

INFORMACIÓN

FACILITACIÓN

[6] Kahnbach L, Lehr D, Brandenburger J, Mallwitz T, Jent S, Hannibal S, Funk B, Janneck M “Quality and Adoption of COVID-19 Tracing Aplicacións and Recommendations for Development: Systematic Interdisciplinary Review of European Aplicacións” J Med Internet Res 2021;23(6):e27989 URL: https://www.jmir.org/2021/6/e27989 DOI: 10.2196/27989

3. Escudo digital: soluciones preventivas
3.1 Rastreo digital de contactos

3.1.1 DP3T (Decentralized Privacy-Preserving Proximity Tracing)

El rastreo digital de contactos ha sido la punta de lanza de la tecnología móvil durante todo 2020. De hecho así se hizo con la creación de protocolos como *DP3T*[7] en el mundo occidental: una solución que permite el desarrollo de aplicaciones de rastreo de contactos mediante el cálculo de proximidad vía *BLE* (Bluetooth Low Energy), variables de tiempo y criptografía de identificadores rodantes, preservando así por completo la privacidad del ciudadano. Este protocolo ha sido publicado y revisado convenientemente[8], demostrando su diseño "*privacy first*" y exponiendo claramente que ningún tipo de dato personal se ve involucrado ni almacenado durante el proceso.

Poco o nada hay que añadir a este protocolo puesto que cumple con lo que promete y ha demostrado ser eficaz para el desarrollo de aplicaciones de rastreo digital. Tanto que gigantes tecnológicos como *Aplicaciónle* y *Google* han facilitado su uso incluyendo en sus *APIs* este mismo protocolo[9,10].

Por último, y en cuanto al *API Aplicaciónle-Google*, exponer que su publicación supuso un movimiento facilitador, que permitió la estandarización de los protocolos en todas las aplicaciones de rastreo digital de contactos que la adoptaron. Tanto a nivel operativo, como técnico.

Dado que el *API Aplicaciónle-Google* no es sino una implementación conjunta de *DP3T*[11], tal y como lo especifica el propio equipo que hay detrás de este protocolo[12], además de cumplir con unos estándares de privacidad previos, esta estandarización hizo posible una mejor interconexión y comunicación entre los países de la *UE*, permitiendo el rastreo unificado mas allá de fronteras políticas.

Por otro lado, no existe una dependencia directa de este *API* para un rastreo digital de contactos adecuado. Una vez adoptado y comprendido el protocolo *DP3T*, la implementación técnica en terminales móviles puede obviar este *API* para centrarse en la capa mas cercana al hardware, y así dejar de depender de un tercero.
Trabajos publicados años atrás, como el de Johan Larsson en 2015[13], hicieron posible un acercamiento a este tipo de tecnologías en terminales móviles mucho antes de la pandemia de 2019-2021, y por lo tanto es posible desarrollar soluciones locales y globales dejando a un lado el *API Aplicaciónle-Google*.

---

[7] Decentralized Privacy-Preserving Proximity Tracing https://github.com/DP-3T/documents

[8] Carmela Troncoso et al. "Decentralized Privacy-Preserving Proximity Tracing" arXiv:2005.12273 https://arxiv.org/abs/2005.12273

[9] Privacy-Preserving Contact Tracing. Aplicaciónle. https://covid19.aplicaciónle.com/contacttracing

[10] Exposure Notifications: Using technology to help public health authorities fight COVID-19. Google. https://www.google.com/covid19/exposurenotifications/

[11] Aplicaciónle. "Aplicaciónle and Google partner on COVID-19 contact tracing technology". 10 Abr 2020 https://www.aplicaciónle.com/newsroom/2020/04/aplicaciónle-and-google-partner-on-covid-19-contact-tracing-technology/

[12] Aplicaciónle/Google exposure notification. https://github.com/DP-3T/documents

[13] Johan Larsson. "Distance estimation and positioning based on Bluetooth low energy technology". 2015. https://www.diva-portal.org/smash/get/diva2:859549/FULLTEXT01.pdf

3.1.2 Otros protocolos

Más allá de *DP3T* y su versión en el *API Aplicaciónle-Google*, existen otros protocolos para realizar un rastreo de contactos digital adoptados en mayor o menor medida en países fuera de la *UE*. Aunque no han demostrado un equilibrio aceptable entre privacidad y eficacia, y algunos de ellos han desaparecido por desuso, es necesario conocerlos para explorar sus capacidades.

Nombre	Obstáculo principal	Referencias
Pan-European Privacy-Preserving Proximity Tracing (PEPP-PT)	Procesamiento de datos centralizado que puede comprometer la privacidad del ciudadano individual	https://en.wikipedia.org/wiki/Pan-European_Privacy-Preserving_Proximity_Tracing
BlueTrace / OpenTrace		https://en.wikipedia.org/wiki/OpenTrace
NHS contact tracing protocol		https://www.nhsx.nhs.uk/covid-19-response/nhs-covid-19-aplicación/
TCN Protocol	Criptografía débil, implementaciones demasiado locales y/o especificaciones privadas o no licenciadas públicamente	https://en.wikipedia.org/wiki/TCN_Protocol
Whisper Tracing Protocol		https://en.wikipedia.org/wiki/Whisper_Tracing_Protocol
Privacy Automated Contact Tracing (East Coast PACT)		https://pact.mit.edu
Privacy-Sensitive Protocols And Mechanisms for Mobile Contact Tracing (West Coast PACT)		https://arxiv.org/abs/2004.03544

3.1.3 Conclusión

El rastreo digital de contactos es la primera pieza de un *escudo digital* destinado a evitar eventos de contagio. Pero más allá de lo eminentemente técnico, una aplicación de rastreo de contactos además de rastrear en función de variables de proximidad y tiempo de exposición, debe poder adaptarse a la realidad científica de una manera ágil.

Es por eso que se han de implementar mecanismos de mejora y mantenimiento continuos para evitar caer en una obsolescencia temprana que la convierta en algo inservible. Los siguientes puntos vienen a describir, una a una, las mejoras y funcionalidades que una aplicación de rastreo de contactos debe de implementar para mejorar su ratio de uso.

3.2 Etiquetado de lugares (venue tagging)

3.2.1 Introducción

El etiquetado de lugares, o *venue tagging*, es una técnica mediante la cual es posible rastrear eventos de contagio en lugares públicos o privados, ya sean cerrados o abiertos, de cualquier dimensión y tipo. De este modo, se podrían detectar deficiencias en la ventilación si hablamos de un espacio cerrado o en medidas de distanciamiento si hablamos de lugares abiertos, entre otras, promoviendo la prevención y evitando así posibles contagios futuros en el mismo lugar.

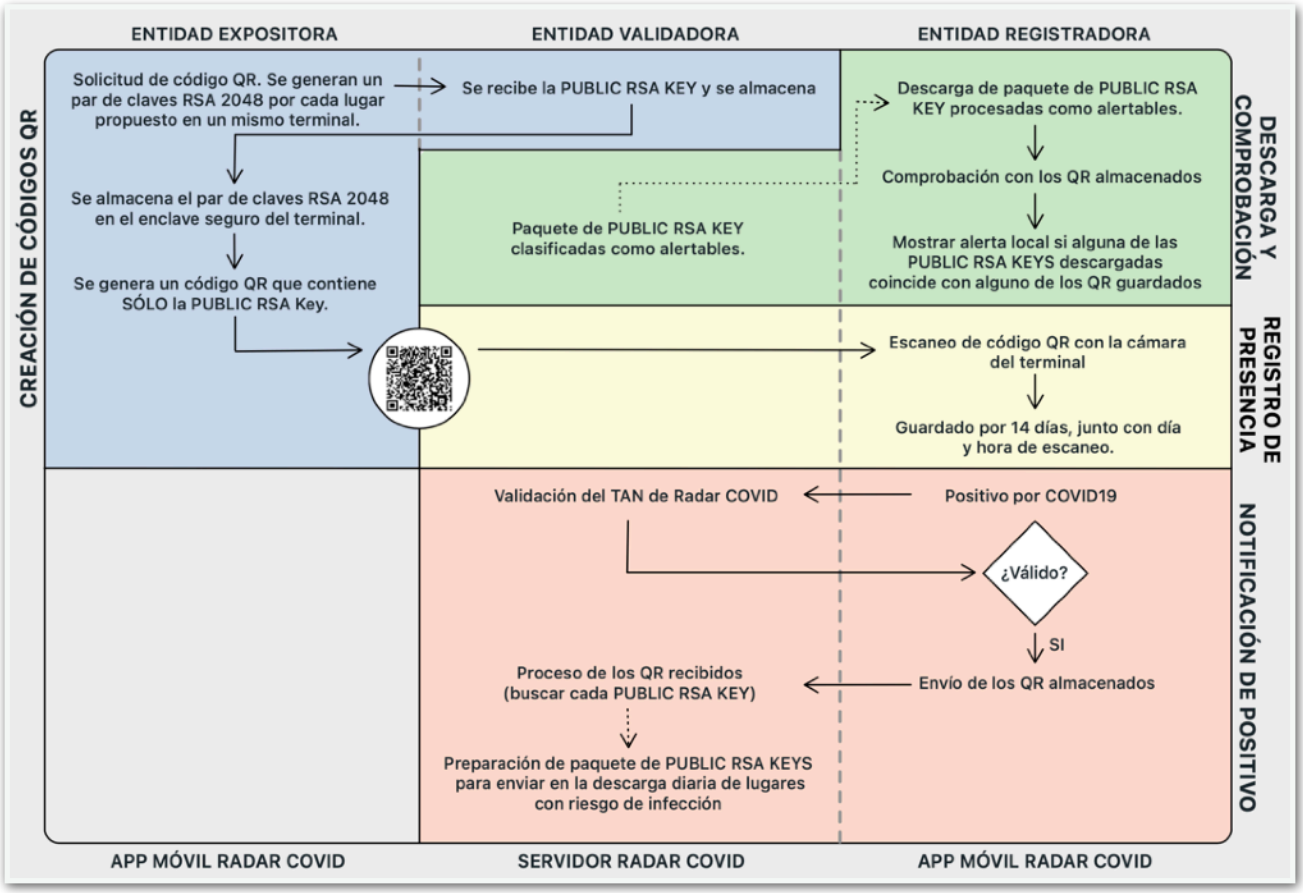
El principio básico de funcionamiento consiste en el etiquetado sistemático de cada uno de los lugares a rastrear mediante códigos *QR*, que deberán ser leídos por la ciudadanía que

acuda a dichos lugares con sus teléfonos móviles. La información contenida en esos códigos *QR*, así como variables de tiempo y fecha, serán claves para determinar la aparición de eventos de contagio masivos en lugares concretos, pudiendo así aplicar protocolos de actuación en estos lugares que acentúen las medidas de prevención.

Se ha dirigido el objetivo hacia los locales de hostelería para aplicar esta técnica, pero igualmente es aplicable a cualquier tipo de evento o lugar en el que se coincidan un número de personas considerable de distinta burbuja social: ascensores, conciertos, oficinas compartidas, coches compartidos, etc.

3.2.2 Propuestas

Durante el invierno de 2020, un grupo de ciudadanos españoles bajo el nombre de *Unidad Tecnológica de Voluntariado*, presentaron un borrador[14] para implementar esta técnica utilizando el mismo transporte e infraestructura que *DP3T*, asegurando así la privacidad de los usuarios y aprovechando el sistema ya implementado para el rastreo de contactos digital.
Dicho borrador está publicado y es de libre acceso, por lo tanto se recomienda su lectura y comprensión.



Esquema de etiquetado de lugares (*venue tagging*) sugerido en Noviembre de 2020 por Jorge J. Ramos y otros a través de *Unidad Tecnológica de Voluntariado*.
Diseñado para ser integrado en la aplicación de rastreo de contactos de España *RadarCOVID*.

Otras sistemas se han propuesto a lo largo del tiempo como por ejemplo *CrowdNotifier*[15]. Aunque versiones recientes de este protocolo ya contemplan un sistema basado en servidor ,

[14] Jorge J. Ramos et. al. "Venue Tagging para Radar COVID". Noviembre 2020. https://github.com/utvoluntariado/utv-propuestas/blob/main/%5BUTV%5D%20Venue%20Tagging.pdf

[15] CrowdNotifier https://github.com/CrowdNotifier/documents

todavía se toman en consideración prácticas como la de dar capacidad a la Autoridad Sanitaria para señalar brotes en lugares concretos.
Algo así supondría una vulneración de la privacidad, puesto que para que para poder señalar un brote en un lugar concreto, la Autoridad Sanitaria debe poseer un identificador único para dicho lugar.
Además, siguiendo el patrón de *CrowdNotifier*, no podría aplicarse *venue tagging* a eventos privados, o lugares que no fuesen de acceso público como ascensores, vestuarios, coches de alquiler por minutos, etc.

Así como el rastreo de contactos digital no requiere mayor colaboración ciudadana que la descarga de una aplicación móvil en un momento determinado, dicha colaboración se vuelve esencial para realizar un etiquetado de lugares (*venue tagging*) eficaz. Para ello, se siguiere el énfasis en los siguientes puntos:

- Evidentemente, y siguiendo el patrón de privacidad primero (*privacy first*) que marca *DP3T*, ni el código *QR* que etiqueta un lugar, ninguna otra variable necesaria, debe identificar unívocamente un usuario o lugar en el tiempo ni el espacio.

- El mensaje debe ser muy claro: al igual que en el rastreo digital de contactos, nunca se utilizarán tecnologías *GPS*, ni cualquier otra u otras tecnologías capaces de ubicar a un particular en un lugar y un momento del tiempo concretos.

Existen antecedentes de éxito de aplicaciones comerciales (Foursquare[16]) que beben de este mismo concepto de etiquetado de lugares (*venue tagging*). Éxito cosechado incluso utilizando explícitamente variables de geoposicionamiento. Aprender cómo éstas empresas incentivaron el uso de sus productos puede ser interesante: beneficios al permitir etiquetado de lugares (*venue tagging*) en negocios, gamificación del sistema, etc.

3.2.3 Mejora continua del sistema

El borrador citado anteriormente[17] presenta una solución de bajo coste y operativa para cualquier persona, negocio y estrato social, pero uno de sus puntos débiles es que el código *QR* que etiqueta un lugar no es rodante (no cambia a lo largo del tiempo de forma desatendida).

Para aquellos lugares que lo soliciten, sería posible implementar un sistema rodante de códigos *QR* que, proyectados sobre cualquier tipo de pantalla, ofrezca un sistema todavía más seguro desde el punto de vista criptográfico. Una revisión de dicho borrador sería necesaria para incluir dicha posibilidad. Técnicamente no reviste ninguna complicación más allá del estándar básico y sería una gran característica a favor de negocios y eventos con mayor capacidad económica, sin perjuicio para los más pequeños.

El etiquetado de lugares (*venue tagging*) se presenta por tanto como una solución eficaz[18] dentro de un conjunto de soluciones y tecnologías destinadas a formar parte de un *escudo digital* completo.

No obstante se ha de insistir una vez mas en la no inclusión de datos personales de ningún tipo o cualquier otro tipo de dato que pueda comprometer la privacidad de los usuarios, como ya ocurrió con la aplicación desarrollada por el *NHS* británico y que tuvo eco en noticiarios

[16] Foursquare. https://foursquare.com

[17] Jorge J. Ramos et. al. "Venue Tagging para Radar COVID". Noviembre 2020. https://github.com/utvoluntariado/utv-propuestas/blob/main/%5BUTV%5D%20Venue%20Tagging.pdf

[18] Wymant, C., Ferretti, L., Tsallis, D. *et al.* The epidemiological impact of the NHS COVID-19 Aplicación. *Nature* (2021). https://doi.org/10.1038/s41586-021-03606-z

de todo el mundo[19]. No obstante aclarar en este punto que los protocolos de revisión por parte de *Aplicaciónle* y *Google*, para el cumplimiento de normativa en cuanto a aplicaciones de rastreo de contactos digital, fueron una barrera eficaz contra este tipo de prácticas, sean intencionadas o no. No es objeto de este informe evaluar o valorar dicha intencionalidad o la ausencia de ella.

Los anexos técnicos de este documento detallan más en profundidad el funcionamiento de este sistema etiquetado de lugares (*venue tagging*) integrado en el propio protocolo *DP3T*.

3.3 Gestión integral de tests

Dado un escenario de emergencia sanitaria mundial, tal y como ocurrió en 2020 a consecuencia de la pandemia de *COVID-19*, resulta imperativo desde el punto de vista epidemiológico mantener una actividad constante de testeo.

La creación de un *escudo digital* debe tener en cuenta el problema logístico y organizativo que conlleva la gestión del testeo y secuenciación continuos de la población, acercando del modo mas eficaz posible la posibilidad a la ciudadania de ser testeada.

Dejando de lado problemas burocráticos, económicos y organizativos que no tienen cabida en este informe, es posible reforzar el *escudo digital* acercando a la población la posibilidad de solicitar tests de forma anónima desde su terminal móvil.

Del mismo modo que utilizamos un vehículo criptográfico en la técnica propuesta anteriormente para el etiquetado de lugares (*venue tagging*), y también para rastrear contactos de forma completamente anónima, podemos utilizar uno para promover el testeo masivo de la ciudadanía, facilitando la solicitud de realización de tests mediante el propio *escudo digital*. Los resultados de dichos tests serán enviados a los terminales móviles que los solicitaron sin comprometer su privacidad.

Todo esto es posible siguiendo un esquema de actuación muy similar al propuesto para el etiquetado de lugares (*venue tagging*), con cuatro procesos clave, y que se detalla en esquema 2 del anexo técnico.

Es importante resaltar que todos los elementos marcados de color azul del diagrama anterior son aquellos que se realizan en el terminal móvil del ciudadano. Observando el diagrama, por tanto, podemos deducir que toda la operativa computacional sensible se realiza de forma descentralizada, quedando relegado el uso de servidores centrales a meros soportes o vehículos de información, pero que por sí mismos no pueden establecer resultados ni relaciones mas allá de lo estadístico.

Sabiendo esto, pasamos a describir cada uno de los procesos:

3.3.1 Solicitar la realización de un test

Cualquier ciudadano desde la aplicación que presenta el *escudo digital*, podría solicitar la realización de un test en su centro mas cercano ya sea este un centro de salud, un puesto temporal montado a tal efecto, etc.

Sería posible solicitar la posición *GPS* del terminal para mostrar al ciudadano cuál es el puesto de testado mas cercano, pero podría ser causa de suspicacias y es mejor evitarlas. Por lo tanto se recomienda la implementación de un sistema de selección de centro de testado vía código postal (introduciéndolo a mano) o simplemente mostrando un listado de todos los centros y facilitar un sistema de favoritos para próximas ocasiones en las que el ciudadano pretenda

[19] BBC. Leo Kelion 12 Abril 2021 https://www.bbc.com/news/technology-56713017?xtor=AL-72-[partner]-[bbc.news.twitter]-[headline]-[news]-[bizdev]-[isapi]&at_custom1=[post+type]&at_custom3=@BBCNews&at_medium=custom7&at_custom4=A1065702-9B71-11EB-975F-DCB94744363C&at_custom2=twitter&at_campaign=64

hacerse un test. En ninguno de los casos esta información saldrá del dispositivo ni se relacionará con él.

Con la información del centro donde se realizará la prueba preferido, se solicitará un turno para realizar el test. En caso de que dicho turno no sea satisfactorio para el ciudadano se podrá elegir un nuevo centro o bien cancelar la operación.

En este primer proceso no se ha comprometido de manera alguna la privacidad del ciudadano. Toda la operación ha sido anónima: se trabaja con identificadores criptográficos únicos gestionados directamente por el ciudadano y pares de claves criptográficas generadas en el mismo terminal del ciudadano.

3.3.2 Realización del test

A la llegada al centro donde se realizará la prueba, un sanitario solicitará al ciudadano el código *QR* que generó durante la solicitud de realización de la prueba. Éste será leído por un terminal preparado para ello, y se comprobará que efectivamente esa persona va a realizarse un test en ese lugar y en ese momento.

En caso de no ser el lugar o la fecha adecuada o no cumplir cualquier otro requisito necesario a posteriori, se invalidará el código *QR* y el ciudadano deberá pedir otra cita, atendiendo a la ocupación y centros disponibles en el momento de la nueva solicitud.

En caso de que se cumplan todos los requisitos para realizar el test, se procederá a su realización. Una vez terminado, se etiquetará debidamente usando una *huella digital*[20] y se preparará para el envío de dicho test a laboratorio.

El etiquetado de los tests puede realizarse mediante impresoras de etiquetas o cualquier otro sistema de marcado que sea capaz de mostrar de manera clara la *clave pública* o *huella digital*, expresada de forma gráfica fisicamente sobre el material que se enviará a laboratorio. En este caso y por el tamaño de las muestras se recomendaría usar códigos "*datamatrix*" o *matriz de datos*, muy extendidos en industria[21].

---

[20] Huella digital de clave pública https://es.wikipedia.org/wiki/Huella_digital_de_clave_pública

[21] Datamatrix o matriz de datos https://es.wikipedia.org/wiki/Matriz_de_datos

3.3.3 Obtención de resultados

Llegadas las muestras al laboratorio se realizará un primer pre-registro de las mismas, escaneando el *datamatrix* de cada prueba y registrando hora y fecha de llegada, así como otros datos como por ejemplo el centro donde se realizó la prueba de origen.

Tras pasar por los procesos adecuados para obtener resultados, éstos se almacenarán en el servidor que gestione el *escudo digital* de tal modo que se disponga de registros del tipo:

43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8	
Puesto de testeo móvil MAD-129*	
SOLICITUD	2021-05-29T07:19:21Z
COMPROBACIÓN	2021-05-29T10:11:21Z
REALIZACIÓN	2021-05-29T10:21:21Z
RECEPCIÓN	2021-05-29T19:03:21Z
PUBLICACIÓN	2021-05-30T08:46:21Z
RESULTADO	POSITIVO

* El nombre del lugar de origen de los tests recibidos puede ser también un *fingerprint* o cualquier otro tipo de clave que oculte el nombre real del lugar.

La figura anterior es tan solo una representación gráfica de un registro de base de datos, pero aporta una visión clara de cómo es posible realizar el trazado completo de un test sin necesidad de utilizar datos personales de ningún tipo.

Estos resultados, o las relaciones entre ellos, deberán ser cifrados convenientemente para que no puedan ser consultados una vez almacenados ni durante la solicitud de los mismos.

3.3.4 Consulta de resultados

Llegados a este punto, y sabiendo que disponemos de una historia prácticamente completa del ciclo de vida del test solicitado, el ciudadano podrá consultar proactivamente el estado de su test desde la aplicación que presenta el *escudo digital*. Éstos resultados se solicitarán al servidor que gestione el escudo digital, utilizando el *fingerprint* creado en el primer paso.

Una vez consultados los resultados, y para cumplir con el principio básico de desmantelamiento elegante (*graceful dismantling*), pasado el tiempo de validez del test que los expertos en la materia marquen como límite según sus propios parámetros (tipo de test, etc), desaparecerán del servidor las *huellas digitales* que clasifican las historias de los tests, quedando sus datos huérfanos, disponibles sólo para análisis estadístico.
No obstante, la aplicación que presenta el *escudo digital* podrá guardar una copia local del histórico de pruebas realizadas, que será completamente irrecuperable en caso de borrado de dicha aplicación.

3.3.5 Conclusiones y aplicaciones derivadas

La digitalización del proceso de testeo de la población a través de la aplicación que presenta el *escudo digital* ofrece una serie de ventajas evidentes:

- Poner a disposición del ciudadano una vía fácil para realizar un test, que junto con la educación e información adecuada redundará en un mayor volumen de testeo.
- Dar al ciudadano el control de todo el proceso, aumentando la confianza en el sistema y demostrando que no es necesario ningún tipo de invasión de la privacidad.

- Unificación de criterios de testado a través de la descentralización del proceso de datos, en la medida que se fomente el uso de este canal para solicitar y realizar tests.
- Obtención de estadísticas en tiempo real acerca de positividad por zonas muy concretas, aunque de nuevo cumpliendo con uno de los pilares básicos del sistema: privacidad primero (*privacy first*).
- Creación de un histórico realista de positividad, facilitando la toma de decisiones y permitiendo a expertos de datos preveer futuros brotes y otras consecuencias derivadas.

En contrapartida, cabe destacar que se requiere una cierta colaboración entre todos los eslabones de esta cadena, lo que nos lleva a tomar la decisión de estar preparados: sistemas como este no pueden escalar de urgencia. Es necesaria una labor sostenida en el tiempo y mantenida por un equipo de profesionales con rotación mínima que establezcan unos criterios técnicos consistentes y unos procesos de implementación adecuados.

Por último añadir que no puede existir una digitalización real del proceso de testeo de la población, sin un plan "analógico" o tradicional que cubra la toma de resultados y los integre en el mismo sistema.

3.4 Herramientas de auto diagnóstico

Mas allá del test clínico fiable capaz de aseverar si un ciudadano está infectado o no, poner a disposición de las personas una guía de auto diagnóstico puede constituir una primera barrera a la hora de hacer cuarentena si fuera necesario o tomar otro tipo de decisiones[22].

Estas herramientas de auto diagnóstico no son sino una serie de preguntas que cualquier ciudadano pueda responder, libremente y el número de veces que quiera, y que concluyen en una recomendación concreta como pueda ser acudir a un centro para realizarse un test, mantener las medidas higiénicas o consultar a un especialista para obtener un mejor diagnóstico.
Por supuesto deberán ser mantenidas y revisadas cada poco tiempo por un equipo médico capacitado, de comunicación y de experiencia de uso.

Como característica principal, las herramientas de auto diagnóstico deben ser auto contenidas. Es decir: no deberán acceder a ningún tipo de máquina o servicio externo para obtener o enviar información de ningún tipo. Además, todo el cálculo necesario para obtener un resultado deberá realizarse en el terminal móvil del ciudadano. Esta característica permitirá utilizar variables de tipo personal como edad, peso o patologías previas, si es que fuesen necesarias para obtener un resultado lo mas preciso posible.

Para potenciar el uso de estas herramientas podrá integrarse un diario de síntomas que muestre el historial de los resultados obtenidos a lo largo del tiempo. Este diario de síntomas se alimentará a través de estas herramientas y sólo mantendrá una copia en el terminal del usuario, que se eliminará al desinstalar la aplicación que gestione el *escudo digital*.

Poner a disposición de los ciudadanos una herramienta fácil de usar y comprender que ofrezca un primer diagnóstico no clínico constituye una manera de potenciar el acceso recurrente a la aplicación que presenta el *escudo digital*, a la vez que se proporciona información muy básica pero muy importante a la hora de identificar y aislar nuevos casos mediante la toma de decisiones personal y privada, informada y avalada médicamente.

---

[22] Kahnbach L, Lehr D, Brandenburger J, Mallwitz T, Jent S, Hannibal S, Funk B, Janneck M "Quality and Adoption of COVID-19 Tracing Aplicacións and Recommendations for Development: Systematic Interdisciplinary Review of European Aplicacións" J Med Internet Res 2021;23(6):e27989 URL: https://www.jmir.org/2021/6/e27989 DOI: 10.2196/27989

3.4.1 Tests de autodiagnóstico

Recientemente[23] ha sido regulada en España la venta de tests de autodiagnóstico sin receta para COVID-19. Estos tests proporcionan una manera sencilla y rápida de esclarecer dudas acerca de posibles contagios, y por tanto cualquier ciudadano puede tomar medidas preventivas en caso de resultar positivo.

Estudios publicados en Julio de 2021[24] han demostrado que el potencial de los tests de antígenos pueden tener un alto rendimiento diagnóstico con pocos casos de falsos positivos entre pacientes asintomáticos.
Sabiendo esto, parece imperativo añadir al rastreo digital esta capa de testeo que cualquier ciudadano puede hacer en la intimidad de su casa.

Siguiendo la idea de tratar los códigos de control para el rastreo digital como recetas, y que por tanto los médicos puedan expedirlos, los farmacéuticos podrían jugar el mismo papel en este caso: si el resultado del test es positivo, el farmacéutico podrá expedir un código para introducir en la aplicación que presenta el *escudo digital*, y así comenzar el ciclo de rastreo de contactos proporcionando una capa mas al rastreo digital estándar y al *venue tagging*.

En este punto es importante tener el cuenta que, siguiendo el método de tratar los códigos de control como recetas, es la Administración Pública la que mantiene la responsabilidad sobre los mismos. Distribuir ésta responsabilidad, permitiendo que empresas privadas o cualquier ciudadano puedan generarlos y expedirlos, puede conducir a usos malintencionados de esta medida y alcanzar niveles de gravedad tales como para bloquear todo el sistema.

Sabiendo esto, el principal problema se encuentra en cómo puede un farmacéutico expedir un código y comprobar la positividad de un tests, si una persona contagiada debe permanecer en cuarentena. La solución que se plantea en este informe pasa por modificar las cadenas de fabricación de dichos tests con el siguiente planteamiento:

- Los tests deberán poder auto validarse contra el fabricante de los mismos, siendo éste el responsable único de la calidad de dicha validación.

- Para ello, se propone modificar la tira reactiva de cada test, para que, en lugar de mostrar una o dos franjas de color, muestre solo en el caso de ser positivo una clave única para poder validarlo. De nuevo, aquí será responsable el fabricante de proporcionar robustez suficiente a su sistema de validación.

- Si un ciudadano realiza su test de antígenos y da positivo, podrá ver dicha clave y proporcionarla al farmacéutico o el responsable de la expedición de códigos de control para el rastreo digital. Junto con el fabricante, el sistema podrá validar la positividad de dicho test y así expedir un código válido.

- El ciudadano introduciría dicho código en la aplicación que presenta el *escudo digital* y así comenzaría el ciclo de rastreo.

Las limitaciones y problemas de esta vía son evidentes, puesto que tratar con la cadena de producción de empresas privadas no será sencillo. Pero a través de la implantación de este sistema como estándar europeo, sería posible añadir una capa más al rastreo digital. En este

[23] Real Decreto 588/2021, de 20 de julio, por el que se modifica el Real Decreto 1662/2000, de 29 de septiembre, sobre productos sanitarios para diagnóstico «in vitro», con objeto de regular la venta al público y la publicidad de los productos de autodiagnóstico de la COVID-19. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2021-12156

[24] Jonas Wachinger, Ioana Diana Olaru, Susanne Horner, Paul Schnitzler, Klaus Heeg, Claudia M. Denkinger, The potential of SARS-CoV-2 antigen-detection tests in the screening of asymptomatic persons, Clinical Microbiology and Infection, 2021, ISSN 1198-743X, https://doi.org/10.1016/j.cmi.2021.07.020. (https://www.sciencedirect.com/science/article/pii/S1198743X21004122)

caso concreto una capa importantísima porque serían los propios ciudadanos los que, activamente, estarían aportando información muy valiosa de positividad en la población.

3.5 Protocolo estándar de medición de CO_2

Durante emergencias sanitarias en las que la transmisión aérea es la principal vía de contagio, la medición de CO_2 en lugares cerrados resulta vital para prevenir eventos masivos y brotes[25].

Existen en el mercado multitud de medidores de CO_2 con mayor y menor sensibilidad que resultan adecuados para entornos domésticos. Para entornos profesionales y públicos, tales como oficinas, aulas, fábricas o locales de hostelería, se antoja necesario un estándar de fabricación, sensibilidad y tipo de sensor de CO_2 para conseguir cierta uniformidad en la medición, en cualquier lugar donde se realice.

Si esta regulación de los aparatos de medición de CO_2 se materializa, resultaría muy interesante la creación de un estándar de comunicación inalámbrico unidireccional, de tal modo que la aplicación que presenta el *escudo digital* sea capaz de recibir y mostrar la medición de CO_2 en tiempo real de aquellos medidores presentes en espacios cerrados no privados, como los citados anteriormente.

Ya existen protocolos estándar de comunicación para los elementos que constituyen el llamado "*hogar inteligente*", como bombillas, cerraduras o altavoces inteligentes. *ZigBee* ha sido durante años el estándar dominante. En el momento de escribir este informe, las grandes empresas y fabricantes están impulsando un nuevo estándar de comunicación llamado *matter*[26] que pretende precisamente encontrar un punto de encuentro entre todos ellos.
La implementación de este estándar, avalado por la *Connectivity Standards Alliance*[27], en todos los medidores de CO_2 que cumpliesen el estándar de fabricación constituiría una importante red de medición de la calidad del aire.

De este modo, cualquier ciudadano desde cualquier lugar, podría consultar en la aplicación que presenta el *escudo digital* la medición de CO_2 antes de acudir a un lugar público concreto, reduciendo así la probabilidad de aglomeraciones y por lo tanto de eventos masivos de contagio.

Así mismo, una detección temprana de una tendencia a superar los límites salubres de concentración de CO_2 en lugares concretos, permitirá tomar decisiones preventivas que favorezcan una mejor ventilación, que pueden ir desde abrir una ventana de forma tradicional, a la automatización completa de la ventilación de un edificio.

4. Escudo digital: soluciones informativas

4.1 Monitores epidemiológicos en tiempo real

Un monitor epidemiológico en tiempo real, es un indicador fiable de la situación epidemiológica de una región, y que muestra datos útiles y en un formato comprensible para la ciudadanía. Este monitor se alimentaría de los datos anónimos contenidos en el servidor que gestiona el *escudo digital*, y aportados tanto desde la aplicación que presenta el *escudo digital* como desde las alternativas tradicionales sugeridas y otras fuentes clásicas.

Un monitor epidemiológico tipo, podría mostrar las siguientes variables atendiendo a cada una de las soluciones que componen las soluciones preventivas del *escudo digital* propuesto, y a otras:

---

[25] Zhe Peng and Jose L. Jimenez. "Exhaled CO2 as a COVID-19 Infection Risk Proxy for Different Indoor Environments and Activities" Environmental Science & Technology Letters 2021 8 (5), 392-397 DOI: 10.1021/acs.estlett.1c00183

[26] matter https://buildwithmatter.com

[27] Connectivity Standards Alliance https://csa-iot.org

1. **Rastreo digital de contactos**
    a. Número total de contagios informados por esta vía
    b. Número total de posibles contagios detectados por esta vía
    c. Número de notificaciones de contacto estrecho enviadas por cada caso positivo
    d. Relación de casos evitados por cada ciudadano que usa el *escudo digital*[28]

2. **Etiquetado de lugares (*venue tagging*)**
    a. Número total de posibles contagios detectados por esta vía
    b. Total de lugares etiquetados con este sistema

3. **Gestión integral de tests**
    a. Número de tests realizados por esta vía
    b. Índice de positividad detectada por cada centro donde se realizará la prueba, sea móvil o fijo.
    c. Índice general de positividad en todo el territorio cubierto por el *escudo digital*

4. **Derivados de otras fuentes**
    a. Carga sobre el sistema de salud
    b. Mapa de concentraciones de CO_2 en lugares públicos
    c. Estadísticas de ocupación contra niveles de CO_2 en lugares públicos
    d. Otros

Disponer de todos estos valores e índices, y otros, para ponerlos a disposición de expertos en explotación de datos, junto con la documentación detallada acerca de cómo se obtienen, es clave para buscar la mejora continua del sistema.

Éstos indicadores, trabajados y expresados de un modo accesible y comprensible, se mostrarán en la aplicación que presenta el *escudo digital* de tal modo que constituya una vía de información eficaz que contribuya a una toma de decisiones convenientemente informada, fomentando una vez mas su uso continuado por parte de la ciudadanía[29].

4.2 Canales de información epidemiológica

Los valores objetivos en tiempo real ofrecidos en el punto anterior son, sin duda, clave para obtener una visión realista de la situación epidemiológica en un territorio. Pero más importante es todavía que la ciudadanía comprenda que significan y porqué son importantes.

Es por ello que la aplicación que presenta el *escudo digital* se postula como una de las vías adecuadas para transmitir conocimientos epidemiológicos a la ciudadanía de una manera clara y fácilmente comprensible. Es importante mantener entre la población un nivel general de conocimientos epidemiológicos lo mas elevado posible, para prevenir así la proliferación de informaciones falsas y por ende la manifestación de comportamientos poco adecuados para frenar cadenas de contagio.

Ésta información deberá ser mantenida por equipos competentes en la materia, así como expertos en otros campos como comunicación y experiencia de usuario.

4.3 Canales de comunicación institucional

Del mismo modo que la aplicación que presenta el *escudo digital* es una vía importante para la educación epidemiológica de la ciudadanía, también lo es para la comunicación institucional a todos los niveles.

---

[28] Wymant, C., Ferretti, L., Tsallis, D. *et al.* The epidemiological impact of the NHS COVID-19 Aplicación. *Nature* (2021). https://doi.org/10.1038/s41586-021-03606-z

[29] Kahnbach L, Lehr D, Brandenburger J, Mallwitz T, Jent S, Hannibal S, Funk B, Janneck M “Quality and Adoption of COVID-19 Tracing Aplicacións and Recommendations for Development: Systematic Interdisciplinary Review of European Aplicacións” J Med Internet Res 2021;23(6):e27989 URL: https://www.jmir.org/2021/6/e27989 DOI: 10.2196/27989

Sin perjuicio de los canales tradicionales de comunicación (radio, televisión, paneles de carretera, etc) la aplicación que presenta el *escudo digital* tiene la capacidad de convertirse, potencialmente, en un medio de comunicación mas inmediato y eficaz, dada la naturaleza de un terminal móvil y los hábitos de utilización[30].

Disponer de una explicación clara y concisa de las restricciones en vigor, ya sean locales, regionales o nacionales, un resumen acerca de quién y cómo puede acceder a ayudas económicas o aclaraciones acerca de cómo se gestionan fondos públicos, proporcionará de manera casi instantánea un crecimiento de la confianza ciudadana a través de la transparencia, así como un mayor uso de la aplicación que presenta el *escudo digital*[31].

Sería ideal la inclusión de sistemas de chat en tiempo real para en la aplicación que presenta el *escudo digital*, además de los métodos clásicos de comunicación como email, teléfono, etc.

4.4 Adaptación de contenidos y funcionalidad

Todas las medidas preventivas descritas anteriormente deben de estar adaptadas a personas con discapacidades visuales, auditivas y motoras para así facilitar el acceso universal a estas herramientas. Los sistemas operativos mayoritarios (*iOS* y *Android*[32]) ponen a disposición de los desarrolladores y diseñadores de aplicaciones móviles, herramientas y guías de estilo para conseguir este objetivo.

Desde hace años, las personas que sufren este tipo de discapacidades pueden utilizar de un modo eficaz dispositivos móviles gracias a estas herramientas. Debido a la naturaleza de la aplicación que presenta el *escudo digital*, se hace completamente necesario diseñar su funcionalidad y contenidos de tal modo que la mayor parte de la población pueda acceder a ellas, y esto incluye a estas personas.

5. Escudo digital: soluciones facilitadoras

El tercer gran bloque de soluciones lo conforman todas aquellas técnicas y sistemas que permitan amortiguar las consecuencias sociales más graves que derivan de una crisis sanitaria global, y cuyo mayor exponente es el confinamiento domiciliario.

Ya sea general o por unidad convivencial, el confinamiento conlleva una serie de daños colaterales, especialmente en hogares familiares con hijos en edad escolar y/o ancianos. Si bien la tecnología no puede construir una solución completamente eficaz para evitar todos estos problemas, si puede aportar soluciones paliativas aceptables o bien vehículos que agilicen procesos de los servicios cotidianos que, en estado de confinamiento, no se pueden realizar de forma normal.

5.1 Sistemas de educación a distancia

Uno de los problemas no sanitarios más graves durante los peores momentos de confinamiento durante la pandemia de *COVID-19*, fue el provocado por la brecha digital en algunos lugares, y que repercutió directamente en la población en edad escolar. Algunos estudios[33] ponen de manifiesto este problema.

---

[30] Cisco Annual Internet Report (2018–2023) White Paper https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html

[31] Kahnbach L, Lehr D, Brandenburger J, Mallwitz T, Jent S, Hannibal S, Funk B, Janneck M “Quality and Adoption of COVID-19 Tracing Aplicacións and Recommendations for Development: Systematic Interdisciplinary Review of European Aplicacións” J Med Internet Res 2021;23(6):e27989 URL: https://www.jmir.org/2021/6/e27989 DOI: 10.2196/27989

[32] Mobile operating systems' market share worldwide from January 2012 to January 2021 https://www.statista.com/statistics/272698/global-market-share-held-by-mobile-operating-systems-since-2009/

[33] Rodicio-García , M. L. ., Ríos-de-Deus, M. P. ., Mosquera-González, M. J. ., & Penado Abilleira, M. . (2020). La Brecha Digital en Estudiantes Españoles ante la Crisis de la Covid-19. *Revista Internacional De Educación Para La Justicia Social*, *9*(3), 103–125. https://doi.org/10.15366/riejs2020.9.3.006

En lugares como Madrid, se intentaron escalar herramientas como *EducaMadrid*, aunque sin mucho éxito debido a múltiples problemas de mantenimiento, integración y funcionales. Aunque con un recorrido de al menos 13 años en el momento de escribir este informe[34], la realidad es que el despliegue y desempeño de esta plataforma ha sido insuficiente y plagado de problemas[35]. Disponer de una plataforma con un recorrido tan dilatado en el tiempo y que no sea operativa cuando se requiera su uso de manera intensiva supone un fracaso indiscutible.

Es una práctica habitual en consultoría de software pública delegar algunas o todas de las funcionalidades *core* o principales, en soluciones prefabricadas de software de código abierto o de terceros (como *Jitsi*, por ejemplo). Esto provoca una mala calidad del software resultante, y muy probablemente muchos problemas de integración y una falta de mantenimiento alarmante.

Debido a la inexistencia de un software público capaz de soportar la carga que supone que toda la formación dejase de ser presencial, muchos centros educativos optaron por tomar decisiones adaptándose a la realidad de cada aula o incluso de cada alumno. Y no siempre con las herramientas más adecuadas[36]. Incluso algunas empresas privadas tomaron iniciativas, aunque quizá algo tarde, para paliar esta falta[37].

Lo que se propone desde este informe es trabajar directamente con los protocolos que hacen posible herramientas prefabricadas como *Jitsi* que, si bien son excelentes para ciertas situaciones y escenarios, quizá no lo sean tanto para este caso concreto donde se tiene que soportar la educación a distancia de todo un país, y se debe controlar cada elemento del sistema.

WebRTC[38] es un estándar de comunicación que comenzó su desarrollo en 2011 y está avalado por la *W3C* y la *IETF*[39] desde el 26 de Enero de 2021. Como todos sabemos, los procesos de estandarización y aval se suelen alargar mucho en el tiempo, precisamente para asegurar que la adopción del estándar es adecuada.

Software como *Jitsi*[40] y otros similares, se basan en *WebRTC* y por ello se propone abandonar el software de terceros para realizar implementaciones propias. Trabajando directamente con estándares conseguimos una comprensión completa acerca de cómo funciona el sistema y acerca de cómo podemos resolver los problemas que ocurran durante su vida útil. Además, el mantenimiento de la herramienta se simplifica, consiguiendo así una herramienta estable, escalable en función de la infraestructura disponible y capaz de responder de una manera ágil a los problemas que vayan surgiendo.

5.2 Sistemas de teletrabajo

La adopción de estándares como *WebRTC* abriría las puertas de otros muchos sectores que se vieron afectados durante la pandemia de *COVID-19*. Es evidente que el software por si mismo no tiene la capacidad de solucionar un problema de la vida real en todo su espectro, y el problema laboral es lo suficientemente complejo socialmente como para que entren en juego otros elementos como leyes, decretos y otros que no se discutirán en este informe.

---

34 EducaMadrid http://www.bocm.es/boletin/CM_Orden_BOCM/2008/12/12/2008-12-12_09122008_0224.pdf

35 Caos en Madrid con la educación 'online': veto a Google y 1,2 millones de alumnos ‘colgados' https://www.elconfidencial.com/tecnologia/2021-01-16/educamadrid-david-calle-online-google-colegios-filomena_2909651/

36 Skype, redes sociales, Moodle y WhatsAplicación, las vías para seguir con las clases desde casa en Granada https://www.granadahoy.com/granada/Skipe-Moodle-wasap-clases-casa-Granada_0_1446755544.html

37 Microsoft Teams se pone a disposición de 650.000 estudiantes y 35.000 profesores en la Comunidad de Madrid para continuar aprendiendohttps://news.microsoft.com/es-es/2020/06/01/microsoft-teams-se-pone-a-disposicion-de-650-000-estudiantes-y-35-000-profesores-en-la-comunidad-de-madrid-para-continuar-aprendiendo/

38 WebRTC https://webrtc.org

39 Web Real-Time Communications (WebRTC) transforms the communications landscape; becomes a World Wide Web Consortium (W3C) Recommendation and multiple Internet Engineering Task Force (IETF) standards https://www.w3.org/2021/01/pressrelease-webrtc-rec.html.en

40 Jitsi Meet https://meet.jit.si

No obstante poner a disposición de las empresas mas modestas un sistema público funcional para realizar ciertas tareas básicas del teletrabajo como comunicación y almacenamiento compartido con el nivel de privacidad y confidencialidad requerido, respondería a una estrategia y una intención de digitalización real por parte de la Administración.

A día de hoy, existen en proceso de estandarización y aval por la *W3C* sistemas de almacenamiento confidencial seguro[41] que bien podrían constituir una línea de investigación y desarrollo seria para, en el futuro no muy lejano, poder ofrecer estos servicios a empresas con menos recursos que así lo requieran.

5.3 Sistemas de consulta médica a distancia

Otro de los problemas derivados de la pandemia de *COVID-19* fue la falta de atención médica para otras enfermedades tanto para pacientes crónicos como para nuevos pacientes. Durante los últimos años, la palabra *eHealth* ha ido apareciendo paulatinamente en la sociedad y su uso se está comenzando a regularizar a marchas forzadas.

El concepto *eHealth* es muy amplio e incluye una gran variedad de aplicaciones y servicios posibles. Si bien es cierto que uno de los primeros pasos a seguir para conseguir una sanidad pública digital es la creación de estándares y manuales de implementación eficaces, este informe se centrará en la necesidad de un sistema de consulta remota. Pretender abordar completamente *eHealth* desde una única necesidad es un error y así debe quedar patente. No es, por tanto, la intención de este informe.

No obstante disponer de una plataforma de consulta remota hubiera facilitado el diagnóstico y la atención tanto de pacientes *COVID-19* como pacientes con otras dolencias. Disponer de esta plataforma además permite la diversificación de los recursos permitiendo realizar consultas en horarios no reglados que, aunque por sí misma no constituye una solución ideal ni definitiva, podría permitir que médicos de cualquier lugar pudieran atender a pacientes de cualquier lugar a cualquier hora del día o de la noche.

Tras eliminar la necesidad del desplazamiento y de la localización física, se facilita a los médicos la organización de su propio tiempo en emergencias de este tipo, pudiendo decidir la forma en que los equipos rotan para atender emergencias como *COVID-19* y la atención a otras enfermedades y dolencias a través de sistemas digitales.

Evidentemente no todas las consultas se pueden resolver a través de sistemas digitales, sobre todo aquellas que requieran de exploración, palpado o otros métodos diagnósticos en los que el paciente deba estar presente. Pero un sistema planteado así puede ofrecer un primer cribado importante, agilizando así el proceso de consulta y diagnóstico, y liberando horarios para el personal médico.

5.4 Sistemas de distribución de bienes de primera necesidad

Otro punto más que nos dimos cuenta que debíamos mejorar durante las fases mas duras de la pandemia de *COVID-19* fue el comercio electrónico. Son de sobra conocidas y usadas por todos los ciudadanos las plataformas de *eCommerce* de grandes supermercados que sufrieron saturaciones y caídas constantes.

Durante los últimos años se han hecho muy populares también aplicaciones de mensajería de proximidad, aplicadas sobre todo al reparto de comida cocinada a domicilio. Últimamente estas empresas están explorando otras vías de negocio, como el de la recogida y transporte de bienes de cualquier tipo como artículos de higiene, bebidas y otros. Incluso empresas dedicadas al transporte de personas han comenzado a aceptar paquetería local[42]. Existen también

---

[41] Confidential Storage 0.1 https://identity.foundation/confidential-storage/

[42] Cabify envíos https://cabify.com/es/empresas/envios

aplicaciones especializadas concretamente en realizar “la compra” y llevarla a casa[43]. En el momento de escribir este informe, se encuentran en fase de implantación otras aplicaciones[44] que prometen “la compra” en 10 minutos, reforzando todavía mas el concepto de mensajería de proximidad.

Pero el problema de todas ellas reside en que solo están presentes en grandes núcleos de población debido a que el mayor volumen de negocio reside, precisamente, en estos lugares. Con esta realidad, parece que pensar en un sistema de mensajería de proximidad público tiene cierto sentido.

La idea básica que se plantea consiste en un sistema de mensajería de proximidad, accesible desde la aplicación que presenta el *escudo digital*, en donde los ciudadanos menos vulnerables puedan ofrecerse voluntariamente para realizar las tareas de adquisición de bienes de primera necesidad en lugar de aquellos ciudadanos que, debido a su situación (mas riesgo, avanzada edad) no puedan, o no deban salir de casa.

Ésta no es una idea nueva, ya que surgió espontáneamente en muchos lugares durante la pandemia de *COVID-19*[45,46,47]. Es necesario, por lo tanto, aprender de esta reacción ciudadana y facilitar el proceso con una herramienta tecnológica a la altura, que ofrezca un canal de comunicación único oficial entre voluntarios y necesitados.

Aunque no ha trascendido ninguna noticia relacionada con robos utilizando la incapacidad de algunas personas para desplazarse a realizar sus compras durante el confinamiento, parece lógico pensar en algún modo que proteja a los ciudadanos mas vulnerables contra estos actos poco éticos. El sistema debería indicar una serie de instrucciones básicas acerca de cómo realizar el acto de entrega y pago de los bienes.

Debido a la naturaleza *privacy first* del *escudo digital* propuesto, no sería adecuado identificar a los voluntarios de ninguna manera: ni fotografías, ni nombres, ni direcciones. Por lo tanto se ha de buscar un método que ofrezca un mínimo de seguridad al ciudadano solicitante y que, por otro lado, pueda ofrecer pruebas policiales irrefutables en caso de que se produzca un delito.

Se propone la implementación, en la aplicación que presenta el *escudo digital*, de un canal de audio y vídeo privado entre solicitante y voluntario (*WebRTC*), mediante el cual el solicitante pueda observar cómo se realiza la entrega en la puerta de los productos solicitados, por parte del ciudadano voluntario.

Antes de la utilización del servicio se expondrán una serie de recomendaciones de uso, y además el solicitante podrá elegir cómo quiere que se le entreguen los productos y cómo realizar el pago: dejar la bolsa en la puerta, pagar una vez recogida la bolsa, que el voluntario permanezca en el descansillo de la escalera, etc.
Éstas recomendaciones deberían incluir no llevar la cara cubierta por parte del voluntario, y solicitar activamente el descubrimiento de ésta por parte del solicitante.

Así mismo, se proveería de una función de grabado de esta comunicación audiovisual en el terminal del solicitante, que sirviese como prueba en caso de allanamiento o robo. Evidentemente, el voluntario sería avisado en su terminal de que su comunicación está siendo

---

[43] Lola Market https://lolamarket.com

[44] Gorillas.io https://gorillas.io

[45] “No salgas, te hago la compra” https://www.lavanguardia.com/madrid/20200314/474118988107/no-salgas-te-hago-la-compra-redes-vecinales-de-urgencia-ante-el-virus.html

[46] “La solidaridad se abre paso en tiempos de coronavirus” https://www.rtve.es/noticias/20200314/no-salgas-hago-compra-solidaridad-se-abre-paso-tiempos-coronavirus/2010052.shtml

[47] “Operación vecino: cuando la atención en cadena es solidaria e inmediata” https://elpais.com/espana/madrid/2020-04-04/las-nueve-magnificas.html

grabada. Esta grabación sería eliminada del terminal del solicitante en el momento en el que confirmase la entrega adecuada de sus productos de primera necesidad.
Éste canal de comunicación sería de utilidad también durante la compra de los productos en el caso de que surjan dudas o alguno de ellos no esté disponible.

En el caso no deseable de que se utilizase esta herramienta como vehículo delictivo, estaría en manos del solicitante enviar la grabación realizada a la policía, identificando así al sospechoso.

El objetivo es establecer una relación de confianza entre solicitante y voluntario, brindando un canal de comunicación privado entre ambos, que en caso de necesidad pueda ser utilizado como prueba ante un juez, disuadiendo así de posibles usos no adecuados de la herramienta.
Los detalles de implementación, el modo en el que se respeta la privacidad tanto del solicitante como del voluntario, y una propuesta del flujo del aplicativo, deberán se expuestos en fases pre-desarrollo.

5.5 Atención psicológica

La pandemia de *COVID-19* ha provocado en ciertos sectores de población una serie de trastornos psicológicos[48] pasajeros o recurrentes que tampoco pudieron tener la atención necesaria por parte de los profesionales adecuados.

Los trastornos mas pasajeros o leves quizá podrían haberse solucionado si hubiera habido alguien "al otro lado" con quien hablar. Del mismo modo que se ha intentado facilitar la labor de los médicos en consulta, sería posible facilitar la labor de los psicólogos para atender estos casos.

Observando que existe un impacto psicológico importante en sectores de población muy jóvenes[49], y atendiendo a las rutinas y costumbres de estos sectores a la hora de comunicarse[50] parece que ofrecer, además de un sistema de videoconferencia, un sistema de chat en el que al otro lado existan profesionales de la salud mental dispuestos a atender consultas y prevenir ciertas conductas destructivas, tiene mucho sentido.

De nuevo, apoyarse en estándares y no en implementaciones de terceros de éstos estándares es la clave del éxito. Si para videoconferencias hablábamos de *WebRTC* como estándar, si hablamos de protocolos de chat hemos de tener en cuenta *XMPP*[51].

Aunque *WebSocket* también puede ofrecer un canal de chat adecuado, no lo sería para este caso debido a que *XMPP* presenta un modelo completamente descentralizado. En general no existe un sistema mejor o peor, simplemente hay que evaluar las necesidades concretas y aplicar la tecnología mas adecuada. A modo de guía podemos establecer los siguientes pros para cada una de las tecnologías con las que podemos establecer un canal de comunicación de chat:

---

[48] Impacto psicológico del COVID-19: los jóvenes presentan más síntomas de ansiedad, depresión y trastornos somáticos http://www.infocop.es/view_article.asp?id=8833

[49] Espada, José P., Orgilés, Mireia, Piqueras, José A., & Morales, Alexandra. (2020). Las buenas prácticas en la atención psicológica infanto-juvenil ante el COVID-19. *Clínica y Salud*, *31*(2), 109-113. Epub 27 de julio de 2020.https://dx.doi.org/10.5093/clysa2020a14

[50] SOCIAL MEDIA, SOCIAL LIFE. Teens Reveal Their Experiences. Common Sense Media (2018). https://www.commonsensemedia.org/sites/default/files/uploads/research/2018_cs_socialmediasociallife_fullreport-final-release_2_lowres.pdf

[51] XMPP https://xmpp.org

XMPP	WebSockeet
XMPP utiliza una arquitectura descentralizada (abierta a todos los usuarios)	Soporte de grandes empresas
Gran soporte	Intercambio de datos de alta velocidad
Seguridad de primer nivel garantizada	No hay restricciones en el número de sesiones que se pueden ejecutar en cualquier momento
Flexibilidad adicional (plugins y mantenimiento futuro)	Los usuarios pueden crear servidores entre dominios

Debido a esta disyuntiva, existen protocolos como el definido por la *rfc7395*[52] que aúna ambas tecnologías y es recomendable su estudio.

6. Conclusiones

La tecnología no es sino una herramienta para ayudar a solucionar problemas. En ocasiones la tecnología solo puede ayudar a alcanzar un objetivo, mientras que en otras puede constituir la solución completa al problema planteado.

Lo que no debe ser la tecnología en ningún caso es un objetivo en sí misma. Debido a esta naturaleza, la creación de un *escudo digital* público solo debe tener como objetivo que, cuando sea necesaria su utilización, pueda responder de manera eficaz y resultar verdaderamente útil para ayudar a atajar el problema. Como parte de la solución y no como la solución en sí misma.

Del mismo modo que un cuerpo de bomberos para actuar de urgencia necesita años de preparación y constante mantenimiento, cualquier herramienta digital requiere lo mismo. En el siglo XXI, es necesaria la creación de equipos públicos encargados de crear y mantener las estructuras necesarias para la implementación de un escudo digital eficaz.

Equipos públicos de alta especialización, al día con las tecnologías necesarias y en constante formación y evolución. Equipos cuyo trabajo no se apoye en directrices, metodologías y tecnologías en desuso y sea auditado públicamente. Equipos que ofrezcan una calidad de software acorde con los tiempos que vivimos y por supuesto con una baja rotación: no dependientes de un gobierno concreto.

Por otro lado no sería inteligente desestimar la colaboración externa. Casos como el de Nueva York y sus *Technology SWAT*[53] son un claro ejemplo de cómo contar con el conocimiento y voluntariedad ciudadana y en algunos casos empresarial, puede hacer crecer el músculo de trabajo cuando sea necesario, además de otros muchos beneficios[54].

Mediante las técnicas descritas en este informe, y la inclusión de otras tantas, es posible garantizar la privacidad y seguridad de los ciudadanos, a la vez que se incentiva el uso del escudo digital como lo que es: una herramienta capaz de ayudar a terminar con una situación de emergencia sanitaria grave, sin despreciar otros métodos mas tradicionales que también han demostrado su eficacia.

---

[52] An Extensible Messaging and Presence Protocol (XMPP) Subprotocol for WebSocket https://datatracker.ietf.org/doc/html/rfc7395

[53] New York COVID-19 Technology SWAT https://www.ny.gov/programs/new-york-state-covid-19-technology-swat-team

[54] NEW YORK STATE COVID-19 TECHNOLOGY SWAT TEAM. Progress Report. https://www.ny.gov/sites/default/files/atoms/files/SWAT-Progress-Report.pdf

En consecuencia, el uso eficaz de un *escudo digital* permitiría la extracción de datos anónimos que facilitaría la labor de los ingenieros de datos y expertos en conducta humana, para predecir riesgos con un alto índice de fiabilidad, y que las autoridades pudieran tomar decisiones en función de dichas predicciones matemáticas. De hecho, durante toda la pandemia han existido profesionales que, libremente y de forma altruista, se han dedicado a ello con un porcentaje de éxito abrumador[55].
Ignorar a estos profesionales no es sino un error de bulto porque la administración no dispone de ellos, ni de sus conocimientos, para el trabajo diario la comunicación con la población.

Por supuesto, la creación de un *escudo digital* no consiste sólo en tecnología. Son necesarios equipos multidisciplinares capaces de sostener en el tiempo una comunicación sólida y llena de verdad que llegue al ciudadano. Éste es el único camino para que una estrategia digital funcione: necesitamos comunicar más y mejor, explicando al ciudadano cómo funciona el *escudo digital* y porqué está garantizada su privacidad.
La confianza ciudadana es imprescindible y sin ella todo este ecosistema no podrá funcionar. Esta confianza sólo la ganaremos con comunicación veraz, transparencia total real y auditoría pública constante.

En definitiva, si existen equipos como la UME[56] (Unidad Militar de Emergencia), que se preparan durante todo el año para acudir allí donde se les necesite y ser altamente eficaces, ¿porqué no disponemos de un equivalente en tecnología?

55 "Los datos nos ayudan a entender mejor cómo se expande esta pandemia" https://bigdatamagazine.es/los-datos-nos-ayudan-a-entender-mejor-como-se-expande-esta-pandemia

56 UME https://www.defensa.gob.es/ume/

7. Clasificación de los módulos del escudo digital

A modo de resumen y para concretar la totalidad funcional del escudo digital, se presenta este cuadro comparativo con alternativas tradicionales para cada uno de los módulos del escudo digital.

Módulo	Digital	Tradicional	Alternativa
Rastreo digital			Rastreo manual
Etiquetado de lugares (VT)			Rastreo manual
Gestión integral de tests			Solicitud telefónica o presencial
Gestión integral de vacunación			Solicitud telefónica o presencial
Monitores epidemiológicos			Radio, televisión, teletexto, otros
Canales de información			Radio, televisión, teletexto, otros
Canales de comunicación			Radio, televisión, teletexto, otros
Educación a distancia			No conocida
Consulta médica a distancia			Consulta telefónica o a domicilio
Solicitud y distribución de BPN*			Solicitud telefónica
Atención psicológica			Atención telefónica

Anexos técnicos

1. Venue tagging (exposición técnica)[57]
1.1 Exposición original (integración completa con DP3T)

1.1.1 Qué es

Venue tagging es una técnica mediante la cual se puede mantener un registro de los lugares visitados en un intervalo de tiempo, ya sea una cafetería, un evento, un ascensor, un vagón de metro o cualquier otro tipo de lugar cerrado o abierto debidamente etiquetado.

El registro personal y codificado de los lugares que cada persona visita, es crucial para detectar casos de contagio además de los producidos por las variables de proximidad y tiempo de interacción.

1.1.2 Cómo funciona

Para que *venue tagging* funcione, se requiere la participación de tres actores principales:

- **Entidad expositora**: negocios, locales, comunidades de vecinos, ascensores, vagones de metro, taxis... todos aquellos lugares susceptibles de ser fuente de contagio de *COVID-19* por aerosoles.
- **Entidad registradora**: todos los usuarios individuales dispuestos a registrar con su terminal móvil, de manera personal y codificada, aquellos lugares que van visitando más allá de sus casas.
- **Entidad validadora**: Sistema capaz de validar los reportes por positivo en *COVID-19*, y con la autoridad para facilitar los tags o etiquetas para la entidad expositora y para orquestar la información necesaria para generar alertas de posibilidad de contagio.

La *entidad expositora* tendrá la responsabilidad de facilitar un método adecuado para que cada persona pueda registrar de forma individual y codificada, su visita al lugar etiquetado.
Por practicidad y facilidad de uso, un código *QR* sería lo más adecuado, ya sea impreso o proyectado en pantallas de cualquier tipo.
Para generar dichos códigos *QR*, cada entidad expositora dispondrá dentro de la aplicación móvil de un apartado donde dar de alta los lugares que pretenda etiquetar. Una vez generado el código *QR*, podrá acceder a el tantas veces como sea necesario.
Sería conveniente que en lugares o eventos que se desarrollan en interiores se expusieran varios códigos *QR* iguales, de modo que no se produzcan aglomeraciones.

La *entidad registradora* serán todas aquellas personas individuales asistentes a aquellos lugares o eventos que se desarrollen en interiores.
Mediante un apartado concreto dentro de la aplicación que presenta el *escudo digital*, la entidad registradora podrá guardar, de manera personal y codificada, cada uno de los códigos *QR* que las entidades expositoras pongan a su disposición, junto con el día y la hora en la que lo hizo.
Estos códigos *QR* quedarán almacenados junto con la información de la fecha, durante 14 días, tiempo tras el cual serán completamente eliminados del terminal móvil de forma automática.

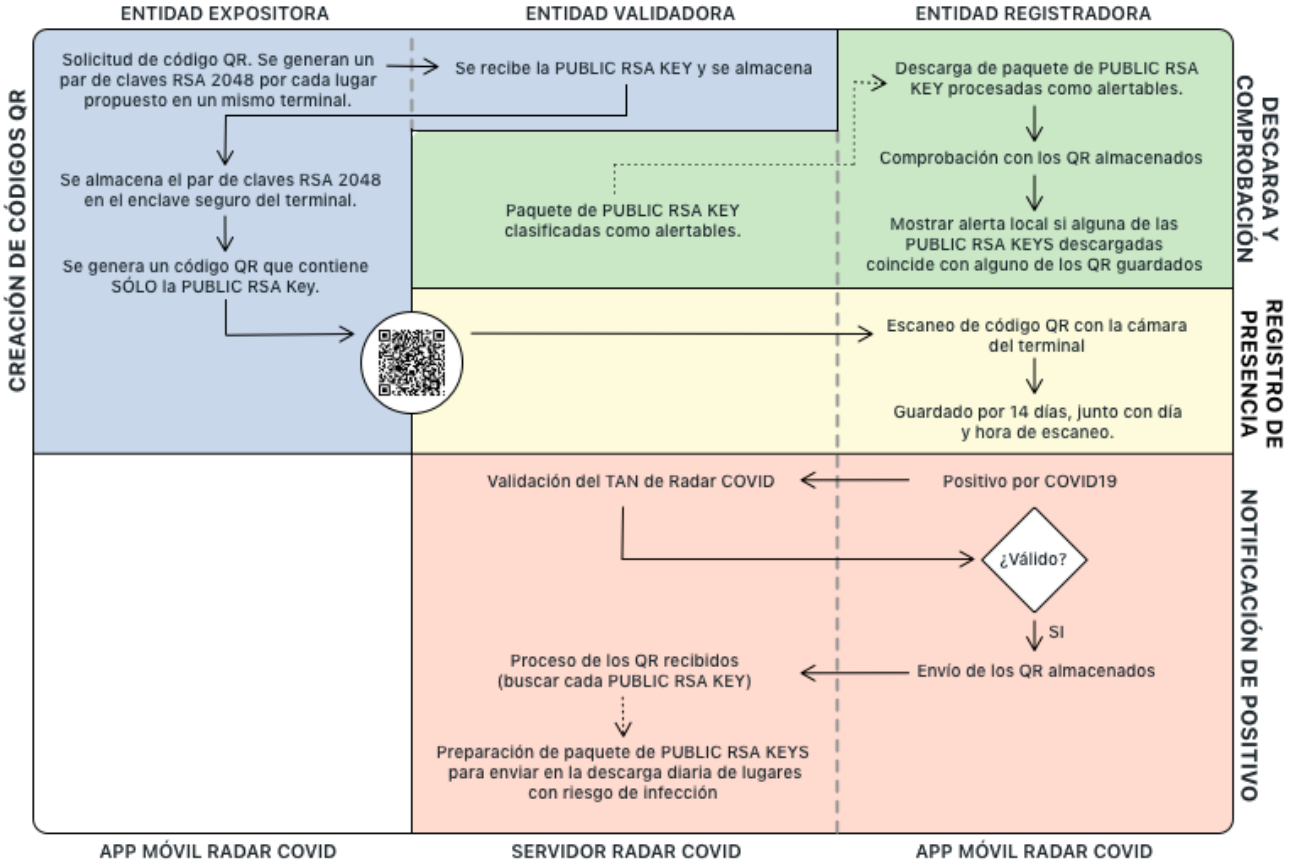
La *entidad validadora* será aquel servidor central responsable de validar los códigos QR generados así como de orquestar el trasiego de información adecuado para generar alertas por posibilidad de contagio de *COVID-19.*
Dado que ya existe un método para validar los reportes positivos por *COVID-19* en aplicaciones de rastreo digital de contactos (como *Radar COVID* en España), presentamos este sistema como un complemento mas, y no como un elemento ajeno a la propia aplicación de rastreo de contactos.

---

[57] Tal y como fue presentada en Noviembre de 2020 por la Unidad Tecnológica de Voluntariado. Se ha realizado alguna modificación gramatical para encajar el texto en este informe.
Jorge J. Ramos et. al. "Venue Tagging para Radar COVID". Noviembre 2020. https://github.com/utvoluntariado/utv-propuestas/blob/main/%5BUTV%5D%20Venue%20Tagging.pdf

A continuación, veremos el esquema completo de la implementación y funcionamiento del sistema.

El esquema 1 muestra el funcionamiento completo del sistema.



ESQUEMA 1: Venue tagging

- A color y en horizontal, se marcan las diferentes etapas del sistema, desde la generación de un código *QR* hasta el reporte de un positivo por *COVID-19*.
- En vertical, los diferentes actores del sistema y la plataforma en la que desarrollan su actividad.
- Las líneas discontinuas muestran el intercambio de información entre los diferentes actores.

Como se puede observar la generación del *QR* sucede siempre en el terminal móvil del interesado, exponiendo sólo la parte pública de un par de claves *RSA 2048*, que será la que dé lugar al código *QR* listo para imprimir o proyectar.

Especial hincapié en el hecho de que la privacidad es una constante durante todo el ciclo del sistema, al seguir el modelo operacional de *DP3T*. Se puede observar también, cómo la integración con aplicaciones de rastreo digital de contactos es completa.

1.1.3 Problemas conocidos

El sistema presenta una objeción principal, que puede ser entendida como un problema por ciertos sectores de la población.

Debido a la naturaleza estática y no rotativa de la clave pública generada para un lugar concreto, se podría proceder a la recogida manual de todos y cada uno de los códigos *QR* generados por el sistema, tan solo recorriendo físicamente los lugares que los presenten.

Habiendo relacionado manualmente cada lugar físico con cada código *QR* generado, y descargando regularmente la información que la aplicación de rastreo digital de contactos ofrecería acerca de los lugares en los que ha estado anteriormente un positivo por *COVID-19*, sería posible saber que locales son aquellos en los que se ha notificado un caso positivo.

Destacar que esta técnica "artesanal" de hackeo del sistema se rompería en el mismo momento en el que se cambiase manualmente uno de los códigos *QR* expuestos.

Esto podría crear suspicacias o llevar a ciertas prácticas de competencia desleal, venganzas u otros comportamientos incívicos.
Pero si entendemos esta información como un dato público, necesario para controlar los efectos de la pandemia en nuestro país, esta "vulnerabilidad" no sería sino una ventaja competitiva para localizar aquellos lugares que no cumplen con las medidas necesarias para evitar contagios y así poder solucionar la situación cuanto antes.

No obstante, el simple hecho de colocar los códigos *QR* en el interior de los lugares interesados eliminaría la capacidad de poder escanear dichos códigos desde la calle, cancelando la mayoría de las posibilidades de explotar esta práctica.

1.2 Revisión (Junio 2021)

Con el ánimo de mejorar el sistema propuesto y evitar la dependencia del flujo de *DP3T* para que, en el caso de que fuera necesario pudiera ser implantado de forma autónoma, se disponen las siguientes mejoras:

1.2.1 Flujo de comunicación independiente

Es posible desacoplar el funcionamiento del sistema *venue tagging* propuesto de *DP3T*, simplemente con imitar su flujo de información. Si trasponemos los actores que entran en juego en *DP3T* y los aplicamos a *venue tagging*, podemos replicar y aprovechar su flujo de información.

No es posible, no obstante, deshacernos de los códigos de control que *DP3T* utiliza para validar los casos positivos. Hacerlo aumentaría exponencialmente las posibilidades de inundar el sistema con falsos positivos, o incluso ataques automatizados que invalidarían el sistema por completo.

Ya que la entrega de códigos de control por parte de autoridades sanitarias no ha funcionado correctamente, atendiendo a los resultados de uso y publicaciones al respecto en prensa técnica especializada[58], será necesario buscar y proponer sistemas alternativos que no dependan de estructuras burocráticas y/o administrativas en cascada.

Tal y como se ha tratado antes en este informe, una gran parte del escudo digital propuesto no puede escalar de urgencia, debido a su naturaleza y complejidad técnica y de implementación. Es por ello que la propuesta ideal pasa por un proceso de estandarización del software sanitario nacional, desempeñado por equipos públicos de baja rotación que desarrollen y mantengan el proyecto a lo largo del tiempo.

Si no es posible un sistema unificado, entonces se podría acudir a algo menos elaborado pero eficaz igualmente: si los médicos ya tienen el control sobre las recetas de medicamentos, ¿porqué no tratar los códigos de control de estas herramientas como tal? Si equiparamos ambos conceptos podemos utilizar los números de colegiado o un carnet digital.

La Organización Médica Colegial de España (OMC), a través de la Entidad de Certificación de la OMC (EC-OMC) tiene autoridad para expedir certificados digitales que corroboran que un

[58] "Nadie supo darme el código", el caos de Radar COVID: códigos que no llegan, notificaciones con retraso y mucho trabajo por hacer https://www.xataka.com/aplicaciones/nadie-supo-darme-codigo-caos-radar-covid-codigos-que-no-llegan-notificaciones-retraso-mucho-trabajo-hacer

médico colegiado lo es[59]. Por lo tanto sería posible utilizar esta certificación para que sean los médicos los que puedan solicitar activamente los códigos de control, a través de una plataforma web segura o la propia aplicación que presenta el escudo digital.

Sería necesario analizar si esta responsabilidad no supondría una carga mayor de trabajo para los médicos y si sería viable.

1.2.2 Uso de fingerprints en lugar de claves públicas completas

El uso de la huella digital de clave pública o *fingerprint*, es un modo más adecuado y simple de administrar estas claves, que simplemente enviarlas o exponerlas públicamente. Encontrar un equilibrio entre la longitud del *fingerprint* y el costo de cálculo sería esencial para acometer esta mejora.

1.2.3 Sistema de identificadores rodantes

Finalmente, una de las mejoras más adecuadas para el sistema *venue tagging* propuesto sería un sistema rodante de pares de claves y, por lo tanto, de *fingerprints*. En aquellos lugares en los que sea posible proyectar un código *QR* en una pantalla, será posible automatizar una rotación de los mismos con la frecuencia que se desee. De este modo se evitan ciertas malas prácticas, y se añade una capa de complejidad adecuada en estos escenarios.
Sería, además, completamente posible atendiendo a cómo *DP3T* maneja los identificadores rodantes de interacción entre terminales móviles

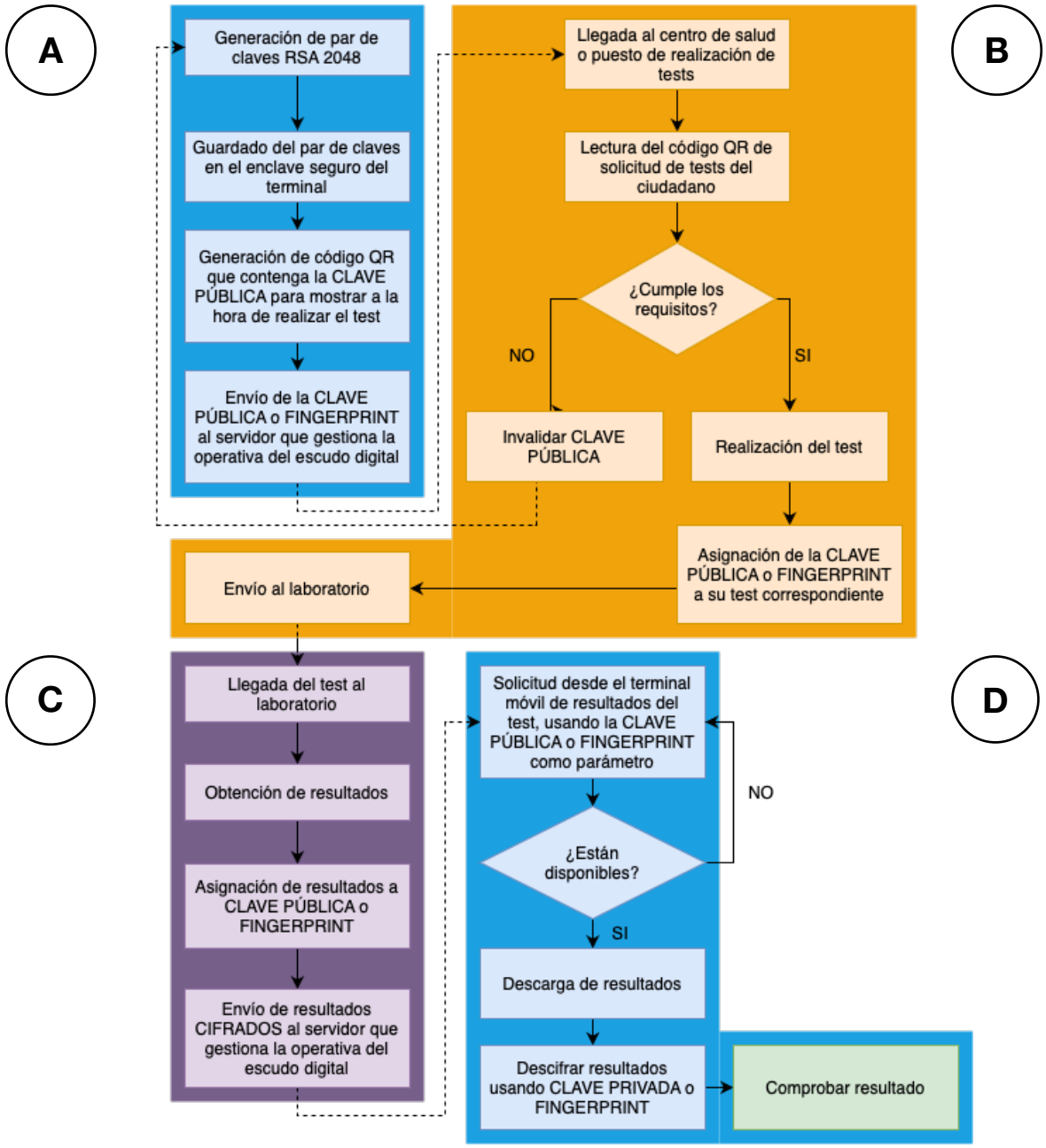
Este sistema de identificadores rodantes puede diseñarse sin perjuicio para aquellos lugares en los que no sea posible proyectar códigos *QR*. En realidad el sistema es el mismo que si se imprimiesen en papel tantos códigos *QR* como se quisiese. Proporcionar un sistema de identificadores rodantes automatizado mejorará la confianza del ciudadano en el sistema y proporcionará una capa adicional de protección al mismo.

Para una implementación correcta es necesario recalcar que ambos sistemas, tanto el *QR* imprimible estático como el *QR* proyectable dinámico, han de poder coexistir sin estar relacionados entre ellos. Cada código *QR*, recordemos, resultado de la generación de un par de claves *RSA 2048* será independiente y deberá ser tratado como tal.

[59] https://certificacion.cgcom.es/node/medico_colegiado_software

2. Gestión integral de tests (exposición técnica)

Siguiendo la estela descrita en la revisión del sistema de *venue tagging* expuesto en este informe, es posible la creación de un sistema que promueva el testado masivo, voluntario y anónimo de la población. Siguiendo el esquema de la figura 2, podemos describir las siguientes etapas:



ESQUEMA 2: Gestión integral de tests

2.1 Solicitud de realización de un test

Una vez se ha seleccionado el centro en el que se realizará, y el día y la hora de la cita, se generan un par de claves *RSA 2048* y se guardan en el enclave seguro del terminal. Tomando la clave pública, el terminal crea un *QR* que posteriormente se mostrará en el centro donde se realizará la prueba. Este código *QR* puede contener además la información de la fecha, hora y lugar donde se realizará el test, aunque no tiene porque estar incluida en la codificación de dicho código *QR*.

Finalmente, se envía la clave pública al servidor que gestiona el escudo digital junto con la información de fecha, hora y centro donde se realizará la prueba. Para asociar la información generada a una clave concreta se recomienda tratar con su huella digital o *fingerprint*[60]. Dado el tamaño de los grupos de población a los que va dirigida el escudo digital, se sugiere el uso de huellas digitales para el intercambio de información.

```
43:51:43:a1:b5:fc:8b:b7:0a:3a:a9:b1:0f:66:73:a8
```

Ejemplo de huella digital o fingerprint

2.2 Realización del test

2.2.1 Interacción ciudadano-sanitario

Cuando el ciudadano llega al centro donde se realizará la prueba, un sanitario leerá el código *QR* directamente desde el terminal del ciudadano, y su información se enviará al servidor que gestione el *escudo digital* para comprobar que efectivamente es correcto.

En caso de no ser el lugar o la fecha adecuada o no cumplir cualquier otro requisito necesario a posteriori, se procederá a invalidar la clave pública que contiene el *QR* y por lo tanto el ciudadano deberá realizar una nueva solicitud. Esto implica el borrado del par de claves del terminal móvil del ciudadano.

Dado que debemos salvaguardar a toda costa la privacidad del usuario, no podemos optar por la notificación *PUSH* para realizar la comunicación que dispare los métodos que borren del terminal del ciudadano el par de claves *RSA 2048* invalidadas.

Por tanto se propone un sistema de comunicación basado en *WebSockets*[61] que, a través de implementaciones o*pen source* como *socket.io*[62], nos permita crear canales de comunicación bidireccionales rápidos, privados y efímeros en aplicaciones cliente / servidor como ésta.

El canal de comunicación se abrirá activamente desde la aplicación que presenta el escudo digital, en el momento de mostrar el *QR* generado y se cerrará al ocultar dicho código *QR*. Pensemos en una ventana modal que muestra y oculta el código *QR* a voluntad del ciudadano. Implementando este sistema estamos dándole el control completo, de tal modo que que será el propio ciudadano el que decidirá cuándo abrir el canal de comunicación con el servidor que gestiona el escudo digital en este punto.

Como no sería posible una comunicación de este modo sin identificar de alguna manera el canal de comunicación en ambas partes, se forzará a que este identificador necesario sea la propia clave pública o su huella digital. Así, además de disponer de un identificador válido para una comunicación efímera como la que necesitamos en este punto, mantenemos la privacidad del ciudadano, al no estar la huella digital ligada a ningún dato personal.
Incluso, para reforzar todavía mas la seguridad, podría establecerse un sistema de identificadores rodantes para los canales de comunicación *WebSocket.*

2.2.2 Envío del test a laboratorio

Una vez realizado el test hay que relacionar de algún modo la muestra tomada con la huella digital del ciudadano cuya clave pública, recordemos, solo está en su poder. Se propone el uso de impresoras de etiquetas *datamatrix*, muy utilizados en industria, aunque depender de un sistema hardware externo puede hacer que el sistema se rompa ante cualquier imprevisto: falta de papel, avería de la impresora, etc.

---

[60] Huella digital de clave pública https://es.wikipedia.org/wiki/Huella_digital_de_clave_pública

[61] The WebSocket Protocol (RFC 6455) https://www.rfc-editor.org/rfc/rfc6455.html

[62] socket.io https://opencollective.com/socketio

Una opción alternativa a la impresión de etiquetas *datamatrix* puede ser la relación digital entre la huella digital del ciudadano y el test realizado. Para ello sería necesario que los tests estuvieran marcados ya de fábrica con un identificador único escaneable, de algún tipo. Así, el proceso de asignar un test a una huella digital de ciudadano simplemente pasaría por escanear ambos.

2.3 Análisis del test realizado

Una vez realizados todos los procesos de laboratorio requeridos para obtener un resultado, se habrá llegado al final del proceso de manipulación del test. Por lo tanto, y en este punto, ya deberíamos tener una historia completa y anónima de dicho test, que podría tener esta forma:

```
{
    "venue": "6b6519f1d8a743a29ab8aa6186e8eba0",
    "request": "2021-05-29T07:19:21Z",
    "verification": "2021-05-29T07:19:21Z",
    "test": "2021-05-29T07:19:21Z",
    "reception": "2021-05-29T07:19:21Z",
    "publication": "2021-05-29T07:19:21Z",
    "result": true
}
```

* Ejemplo JSON con la historia completa de un test

Estos registros deberían guardarse cifrados en base de datos, de tal modo que sólo el ciudadano que posee la clave privada asociada al *fingerprint* de su clave pública, pueda leerlos. Para ello, y al obtener un resultado definitivo para el test, la clave pública del usuario deberá ser utilizada para cifrar toda la historia, comunicarla y desaparecer.

Ningún dato personal ha sido utilizado durante todo el proceso, y además los resultados quedan completamente desprendidos de su relación con el *fingerprint* de la clave pública del usuario, por lo que el testeo permanece completamente anónimo a la vez que se obtienen datos fiables acerca de positividad, eficacia de la red y otros muchos datos estadísticos que puedan ayudar a mejorar los procesos.

2.4 Comunicación de resultados

El ciudadano podrá consultar sus resultados de forma proactiva, es decir, directamente realizando una acción de actualización en la aplicación que presenta el escudo digital. Si la solicitud parte del usuario, evitamos automatizaciones utilizando tecnología *PUSH* que, si bien sería adecuada en otros escenarios, no lo es en este.

El hecho de evitar la automatización de la notificación de los resultados utilizando tecnologías como *PUSH* es intencionado. Un token *PUSH* es capaz de identificar un terminal móvil de forma unívoca y eso comprometería la privacidad del ciudadano.

La alternativa a esta automatización es la notificación local. Tomando en cuenta los datos estadísticos globales acerca de la velocidad de procesamiento de los test en laboratorio, congestión de la red logística que los lleva hasta allí, y otros muchos factores intervinientes un terminal móvil podría localmente hacer los cálculos adecuados para presentar alertas que recuerden al ciudadano que debe consultar el resultado de su test.

2.5 Toma de decisiones

Una vez que el usuario ha solicitado los resultados de sus test y los ha obtenido, esa información deberá se suficiente para que la aplicación que presenta el escudo digital pueda presentar una serie de recomendaciones y medidas a tomar en función de dicho resultado.
Esa información deberá ser actualizada constantemente por equipos competentes, en función de la situación epidemiológica del momento.

Todo este proceso sucede de manera local, en la aplicación que presenta el *escudo digital*. Por lo tanto no hay posibilidad de identificación ni de seguimiento alguno que ponga en peligro la privacidad del ciudadano.

3. Notas finales

Estos anexos técnicos no pretenden ser una guía completa de implementación. Se trata más bien de una primera inmersión teórica en cómo funcionarían los sistemas a este nivel. Existen multitud de detalles de implementación que no se describen en estos anexos, por una razón sencilla: dichos detalles son propios de fases de pre-desarrollo y éste es un informe preliminar que sólo pretende documentar que es posible realizar un escudo digital con las condiciones propuestas.

Quedan fuera de este informe los modelos para integrar de forma segura profesionales de la medicina para servicios como la consulta por videoconferencia o la atención psicológica mediante chat. Aunque se dibuja un modo de hacerlo mediante los certificados digitales que la Organización Médica Colegial de España (OMC), a través de la Entidad de Certificación de la OMC (EC-OMC) expide, queda pendiente de definición en etapas pre-desarrollo.

Del mismo modo, quedan fuera también de este informe las propuestas de implementación para los sistemas de chat y los sistemas de distribución de bienes de primera necesidad por los mismos motivos, en los que se insistirá una vez mas: la intención de este informe no es ofrecer un análisis técnico completo ni constituir una toma de requisitos previa a un desarrollo. Ese trabajo deberá realizarse dentro de un marco de trabajo, por equipos multidisciplinares de analistas.

Sabiendo esto, hemos de ser conscientes de que la calidad del software es *esencial* en un sistema público grande como el que se propone en este informe. Huir de ciertas prácticas muy extendidas hoy en día en la consultoría de software en España es vital para alcanzar cotas de calidad aceptables:

- *Abandonar la adopción de software y soluciones prefabricadas de terceros para crear frameworks propios basados en estándares*. No se trata de reinventar la rueda, pero el uso y abuso de este tipo de software provoca soluciones inestables y altamente dependientes de terceros no interesados.

- *Abrazar prácticas de auditoría pública constante*, mediante la publicación de la documentación y el código fuente que constituye el trabajo realizado.

- *Desechar metodologías de trabajo desfasadas,* como *Métrica3* cuya última versión data de 2001[63] y entierra sus raíces en 1989[64]. Pero no es la edad del *framework* lo que determina su validez, sino su contenido. *Métrica3* constituye uno de los ejemplos más claros de *proyectos en cascada*: poco flexibles y con más documentación de la estrictamente necesaria. Y, si en algún momento surge algún problema no previsto, toda la gestión del proyecto cae. Evidentemente, el software ya no se desarrolla así.

---

[63] Métrica v.3 https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Metrica_v3.html

[64] Métrica https://es.wikipedia.org/wiki/MÉTRICA

Necesitamos implementar metodologías que focalicen mas esfuerzos en la adaptabilidad que en la previsibilidad. Pasada la fiebre *SCRUM*, que erróneamente siempre se asoció como la única manera de implementar *Agile*, *Extreme Programming*[65] se presenta como una de las metodologías mas flexibles y capaz de acelerar los procesos de desarrollo de software, siempre de una forma eficaz, controlada y documentada en su justa medida.

- *Mantenimiento y mejora continua*, que asegure la eficacia del desarrollo cuando se necesite usarlo. El software no es una entidad capaz de sobrevivir mucho tiempo sin actualizaciones. La tecnología avanza continuamente y es por ello que las soluciones de software deben adaptarse al tiempo en el que se las necesita. Es por ello que se requieren de equipos con una baja o muy baja rotación, que mantengan y compartan el conocimiento acerca de las herramientas.

  El modelo actual de licitación y consultoría ha demostrado no ser eficaz a la hora de crear y mantener soluciones públicas de software, debido al modelo de contratación: si se acaba el contrato, se acaba el mantenimiento. No podemos permitirnos algo así en el software público y por eso desde aquí se reivindica la creación de equipos de desarrollo altamente especializados y entrenados en las técnicas descritas, al igual que existen cuerpos especializados en otras disciplinas como la *UME*[66], capaces de intervenir cuando la situación lo requiere puesto que para ello se entrenan durante todo el año.

- *Utilización de las mejores tecnologías a disposición de los desarrolladores*. Vivimos una época dorada para el desarrollo de software que nos permite tomar múltiples caminos para llegar a un mismo lugar. Por ejemplo, podemos realizar aplicaciones móviles utilizando frameworks originalmente pensados para web. Esto es sin duda una ventaja en muchos escenarios, o a la hora de realizar ciertos proyectos. Pero un proyecto público de la envergadura planteada en este documento, requiere de las mejores herramientas disponibles en cada momento y en cada plataforma: apostar por código nativo en plataformas móviles antes que hacerlo por sistemas *cross-platform*[67].

  Si bien es cierto que estos sistemas ofrecen algunos elementos positivos en escenarios concretos como por ejemplo una sola base de código para cualquier plataforma, los contras superan a los pros por muchas razones, pero quizá la mas importante sea que si buscamos rendimiento y estabilidad, tal vez nada pueda ser mejor que una aplicación nativa, porque el código nativo se integrará con todas las API de hardware y aprovechará la mayoría de las capacidades de la plataforma. A largo plazo, mantener dos bases de código también puede ser más fácil que una sola en una aplicación *cross-platform*.

  En términos de negocio, no hay herramientas buenas o malas. Solo hay herramientas diseñadas para resolver tareas específicas. En el caso de los sistemas *cross-platform*, la tarea que resuelven es el desarrollo de aplicaciones en varias plataformas, utilizando tecnologías conocidas. Ayuda a los equipos a ahorrar presupuesto, tiempo y esfuerzo en el desarrollo.
  Pero nada supera a la aplicación nativa en términos de rendimiento y experiencia del usuario. Por lo tanto, y en el caso que nos ocupa, apostar por código nativo no es una elección arbitraria sino una necesidad, porque un escudo digital no puede construirse rápidamente para "parchear" una situación y ***la experiencia de uso es vital*** para obtener la confianza ciudadana.

Superar todos estos escollos no es tarea fácil, pero como sociedad tecnológica hemos de avanzar hacia un modelo de desarrollo de software público eficaz y de utilidad que, indiscutiblemente, pasa por la adopción estas y otras prácticas de probado éxito en la empresa privada y aceptadas por la comunidad de desarrollo.

---

65 Extreme Programming https://es.wikipedia.org/wiki/Programación_extrema

66 UME https://www.defensa.gob.es/ume/

67 Multiplataforma https://es.wikipedia.org/wiki/Multiplataforma