

Reporte Técnico Final

Sistema descentralizado para detectar zonas de riesgo y
contacto con personas confirmadas con COVID-19 protegiendo
la privacidad de los participantes

CONACyT-313572-Applicovid-DT Versión 1.0

Centro de Investigación y de Estudios Avanzados del IPN
Departamento de Computación

1 de diciembre de 2020

Datos del proyecto		
Organización:	Cinvestav	Departamento de Computación
Proyecto:	CONACyT-313572	Sistema descentralizado para detectar zonas de riesgo y contacto con personas confirmadas con COVID-19 protegiendo la privacidad de los participantes
Sistema:	Applacovid	Reporte Técnico Final

Documento		
Clave	Nombre	Versión
DT	Reporte Técnico Final	Versión 1.0

Documentos Relacionados		
Clave	Versión	Nombre
Protocolo	1.0	Propuesta Técnica
DT-AM	1.0	Aplicaciones Móviles
DT-Android	1.0	Android
DT-iOS	1.0	Apple iOS
DT-SIG	1.0	Sistema de Información Geográfica
DT-PW	1.0	Página Web

Firmas		
Responsable Técnico	Colaborador	Colaborador
Dr. Francisco Rodríguez Henríquez Profesor-Investigador Cinvestav	Dra. Brisbane Ovilla Martínez Profesor-Visitante Cinvestav	Dr. Cuauhtémoc Mancillas López Profesor-Investigador Cinvestav

Índice general

1. Descripción del proyecto	1
1.1. Introducción y antecedentes	1
1.2. Descripción general del sistema	2
1.2.1. Objetivo general	2
1.3. Módulos principales del sistema	4
1.3.1. Subsistema: Página Web	4
1.3.2. Subsistema: Sistema de Información Geográfico Web	5
1.3.3. Subsistema: Consola de Administración	7
1.3.4. Subsistema: Aplicaciones móviles	8
1.4. Productos esperados: Entregables	10
1.5. Resultados	11
1.5.1. Resultados obtenidos	11
1.5.2. Perspectivas de desarrollo hacia el futuro	13
1.6. Problemas surgidos y solución de los mismos	14
1.6.1. Ajustes en el presupuesto	14
A. Documentos relacionados	19
A.1. Infografía: “App que avisa de posible contagio”	20
A.2. Carta de apoyo Dra. Álvarez-Buylla dirigida a Google y Apple	21

Índice de figuras

1.1.	Subsistemas que componen a Applacovid	3
1.2.	Marco conceptual del SIGWeb	6
1.3.	Capa de casos confirmados por covid	6
1.4.	Capa de casos negativos por covid	7
1.5.	Capa de casos sospechosos por covid	7
1.6.	Capa de casos de defunciones por covid	8
1.7.	Detección de contactos vía Bluetooth.	9
A.1.	Infografía: "App que avisa de posible contagio"	20
A.2.	Carta de apoyo Dra. Álvarez-Buylla dirigida a Google y Apple	21

CAPÍTULO 1

Descripción del proyecto

1.1. Introducción y antecedentes

El 21 de abril de 2020, el subsecretario de salud Dr. Hugo López-Gatell, anunció a la Nación la entrada en vigor de la fase 3 de la pandemia del COVID-19. Una de las medidas más importantes de ese anuncio fue la recomendación de mantener la *Jornada de Sana Distancia* hasta el 30 de mayo. Debido a las incertidumbres con respecto a la evolución de la pandemia, las medidas de confinamiento fueron extendidas por semanas que se volvieron meses. En estos días finales del mes de noviembre de 2020, con varios Estados con su semáforo en rojo, y con una Ciudad de México al borde de revertir su semáforo color naranja a rojo, las sensaciones son de que la situación de emergencia en todo el país se extenderá [por lo menos] a los primeros meses del año 2021.

Un obstáculo importante para definir con precisión el momento más adecuado para levantar la cuarentena que opera actualmente en México a diferentes niveles, es el riesgo de que el retorno a las actividades normales propiciará, casi irremediablemente, una interacción entre población sana y pacientes confirmados de COVID-19. Es altamente probable que ese desafortunado evento se presente debido a una de las características más inconvenientes de esta enfermedad: los pacientes asintomáticos pueden contagiar a población sana durante un período que va desde pocos días hasta dos semanas. Existe consenso internacional de que una de las medidas más eficaces para reducir los brotes de contagio es la de tener un rastreo efectivo de las redes de contactos de personas recientemente infectadas.

Estamos entonces ante la imperante necesidad de contar con herramientas ágiles y oportunas que permitan notificar a la población mexicana de posibles contactos de riesgo a los que un grupo de personas pudieron estar expuestos en los últimos días, o incluso, en las últimas semanas.

En este proyecto se propone una solución que ayuda a disminuir drásticamente la problemática arriba mencionada. Concretamente, nuestra propuesta toma ventaja de los dispositivos móviles del tipo *smart phone*, los cuales son utilizados masiva y cotidianamente por la población urbana residente en México [5]. Como se explica a continuación, nuestra herramienta informática ofrece una solución descentralizada, práctica, eficiente, y estrictamente respetuosa de la privacidad de los usuarios del sistema.

1.2. Descripción general del sistema

Applacovid¹ es una aplicación móvil para celulares iOS y Android de la gama *smart phone*, desarrollada para ayudar a los usuarios a detectar contactos con contagio COVID-19.

A partir de su descarga, por parte de los usuarios en sus dispositivos móviles, Applacovid genera credenciales seudónimas, las cuales son renovadas periódicamente. Utilizando la tecnología de proximidad Bluetooth, estas credenciales seudónimas son intercambiadas constantemente entre todos los usuarios que estén en contacto cercano al usuario y que, por supuesto, tengan instalada la aplicación en sus dispositivos móviles. Por ejemplo, si dos usuarios (con Applacovid instalada) coinciden en la salida/entrada de una estación del metro o del metrobus, las aplicaciones intercambian los seudónimos de manera multitudinaria. Los seudónimos, al ser recibidos, son almacenados por la aplicación para ser clasificados con respecto a sus metadatos asociados, siendo dos de los metadatos más importantes: la fecha en el instante de la coincidencia; y la proximidad del celular que hizo el envío.

Por otro lado, aquellos pacientes que recién han sido confirmados como casos activos de COVID-19 pueden informarlo oportunamente y de manera voluntaria, a través de una comunicación anónima entre Applacovid y el servidor del sistema². Esta acción permite el servidor hacer público a todos los usuarios, con Applacovid instalada, los seudónimos que pertenecen a personas que han sido confirmados como portadores de COVID-19. Esta información preserva la privacidad de las personas enfermas, puesto que el servidor desconoce las identidades reales de los dueños de tales seudónimos e incluso desconoce con qué seudónimos ha tenido interacción cada usuario ya que esto jamás es transmitido. Finalmente, el ciclo se cierra cuando Applacovid, en cada celular instalado, actualiza su base de datos con los registros de seudónimos más recientes agregados por el servidor del sistema. Applacovid verifica entonces si alguno o algunos de los seudónimos publicados en la última actualización aparecen en la base de datos local, y si fueron recibidos en los últimos días o semanas. De ser así, implica que ese usuario estuvo en contacto cercano con al menos una persona de quien ahora se sabe que es portadora del virus.

Applacovid cifra la información almacenada en el dispositivo y conforme a las políticas de control establecidas, permite que esta información se elimine una vez haya pasado su periodo de uso.

Por otro lado aquellos usuarios que den positivo a la prueba COVID-19 se les proporciona un código único e intransferible, por parte de la Secretaría de Salud. Este código puede ser utilizado para que el usuario se declare así mismo como contagiado ante el servidor del sistema. Este mecanismo evita que personas malintencionadas propaguen información falsa sobre contagios no existentes. De esta manera, sólo los usuarios verdaderamente contagiados tienen permiso de compartir información sobre su contagio con el servidor del sistema.

1.2.1. Objetivo general

Desarrollar un sistema digital descentralizado que notifique a los usuarios sobre contactos cercanos con personas confirmas con COVID-19 y que sea capaz de detectar zonas de riesgos. El sistema deberá preservar el anonimato de las personas portadoras del virus, así como la privacidad de todos los usuarios del sistema.

¹En adelante se usará indistintamente aplicación y/o Applacovid para referirse al sistema.

²También denominado *backend* (BE)



Figura 1.1: Subsistemas que componen a Applacovid.

1.3. Módulos principales del sistema

Applacovid toma ventaja de los dispositivos móviles del tipo smart phone, los cuales son utilizados masiva y cotidianamente por la población urbana residente en México. Nuestra herramienta informática ofrece una solución descentralizada, práctica, eficiente, y estrictamente respetuosa de la privacidad de los usuarios del sistema.

Concretamente el proyecto involucra el uso de las siguientes tecnologías:

- Tecnología de comunicación Bluetooth,
- Lenguajes de programación Java para Android, Objective-C y Swift para iOS
- Sistemas operativos Fedora, ubuntu, ios y Android,
- Base de datos relacionales, incluyendo Oracle y Postgresq
- Manejadores Unity Content Management System (CMS),
- Bibliotecas Apache, SSL/TLS.
- Tecnología Docker
- Herramientas de desarrollo Android Studio y Xcode para iOS
- Otras tecnologías relevantes para este proyecto incluyen: deSpring MVC, HTML, CSS y JS, Plus Spring Boot, Spring Security, Jquery, Thymeleaf.

Applacovid se divide en cuatro subsistemas principales, como se muestra en la Figura 1.1, los cuales interactúan entre sí para complementar la información proporcionada a los usuarios en las aplicaciones móviles y permitir una administración sencilla de los portales web.

- **Página Web:** Es la página web de Applacovid desde la cual se pueden descargar las aplicaciones móviles para iOS y Android. Además, los internautas podrán encontrar información útil para la protección y cuidado ante COVID-19.
- **Sistema de Información Geográfico Web:** El sistema geográfico de este proyecto proporciona información actualizada sobre los contagios de COVID-19 en el país y por municipio. La página web proporciona un acceso directo para la consulta de los mapas.
- **Consola de Administración:** Este sistema permite a una autoridad de salud registrar a un usuario como contagiado ante Applacovid, por medio de su código QR. También permite al administrador del sistema actualizar las noticias y preguntas frecuentes de la página web.
- **Aplicaciones móviles:** Son las aplicaciones móviles para iOS y Android de Applacovid. Es un subsistema independiente de los anteriores ya que está diseñado para responder la alta demanda computacional asociada a las aplicaciones móviles.

1.3.1. Subsistema: Página Web

El sitio web forma parte integral del sistema como se muestra en la Figura 1.1 al satisfacer los siguientes objetivos:

- **Facilitar información:** Proporciona al usuario visitante los datos, ligas e información necesarios para la descarga, instalación y uso de la app *Applacovid*. Se incluye una sección para mostrar las novedades acerca del sistema, así como las preguntas frecuentes acerca de la aplicación.
- **Integración con el Sistema de Información Geográfica Web:** Se visualizan datos geográficos proporcionados por el gobierno federal y estadísticas de interés, relacionadas con la propagación del virus, como son: zonas de riesgo y casos confirmados por estado o municipio, así como el semáforo epidemiológico.
- **Debe ser responsivo:** El término *responsivo* se refiere a que el sitio web debe adaptarse de manera flexible para una correcta visualización en una amplia variedad de dispositivos, con diferentes características y tamaños de pantalla. Para ello se utiliza la tecnología *Bootstrap 4.5* y se mantienen los recursos en línea con un mínimo de requerimientos de ancho de banda y almacenamiento.
- **Respetar la privacidad:** El sitio tiene libre acceso a cualquier internauta, no requiere de ninguna información personal o correo electrónico, no se le envía propaganda o *spam* de ningún tipo. La visita al sitio es totalmente anónima y no se muestra ninguna información sensible o protegida por derechos de autor. Las estadísticas gubernamentales son públicas.

La creación de sitios web comprende una serie de procesos que suelen dividirse en dos grandes etapas: el diseño y la implementación.

Dentro de la etapa de diseño se define, por un lado, la organización de la información que se va a presentar, la cual es hasta cierto punto independiente del apartado gráfico.

Por otra parte, dentro del diseño web se define también lo que se conoce como el diseño gráfico, es decir, la apariencia visual del sitio. En este apartado se incluye la definición de la paleta de colores y la creación de los elementos gráficos tales como íconos, botones, figuras e imágenes que aparecerán en el sitio.

Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte “pagina_web.pdf” .

1.3.2. Subsistema: Sistema de Información Geográfico Web

El sistema de información geográfico web (SIGWeb) está diseñado como una parte integral de la página web del proyecto Applacovid.

El marco general del sistema de información geográfica como una aplicación independiente puede verse de manera conceptual, de modo que en la Figura 1.2, se muestra la vista general de las funcionalidades del SIGWeb.

Funcionalidades principales

Además de la visualización normal de las capas, la búsqueda de datos, panorámica y acercamiento de las capas, se diseñaron las siguientes funcionalidades:

- Control de capas de nivel estatal y municipal de casos covid
- Despliegue de información geo-estadística
- Despliegue de zonas de riesgo acorde a los casos confirmados de covid

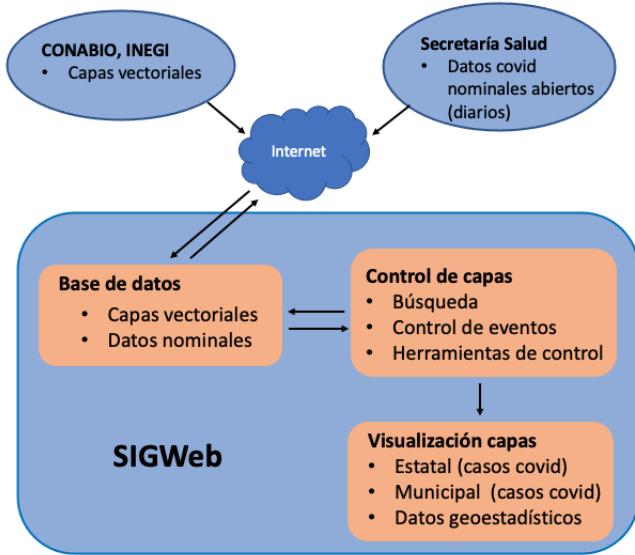


Figura 1.2: Marco conceptual del SIGWeb

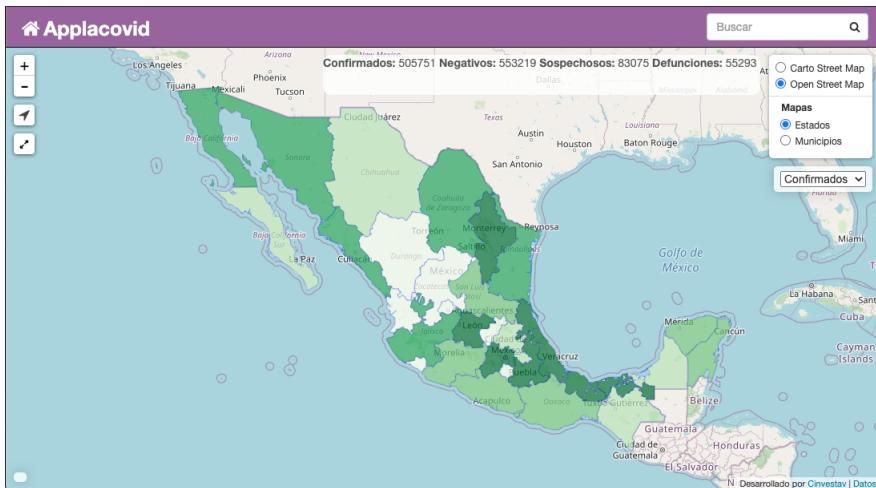


Figura 1.3: Capa de casos confirmados por covid

Al seleccionar la opción de “confirmados”, se despliega una capa de información de casos confirmados con un rango de colores verdes, donde la intensidad más clara indica un número menor casos, y por el contrario, una intensidad mayor indica un número alto de casos confirmados (véase la Figura 1.3).

Al seleccionar la opción de “negativos”, se despliega una capa de información de casos negativos con un rango de colores rojos, donde la intensidad más clara indica un número menor casos, y por el contrario, una intensidad mayor indica un número alto de casos negativos (véase la Figura 1.4).

Al seleccionar la opción de “sospechosos”, se despliega una capa de información de casos sospechosos con un rango de colores naranjas, donde la intensidad más clara indica un número menor casos, y por el contrario, una intensidad mayor indica un número alto de casos sospechosos (veáse la Figura 1.5).

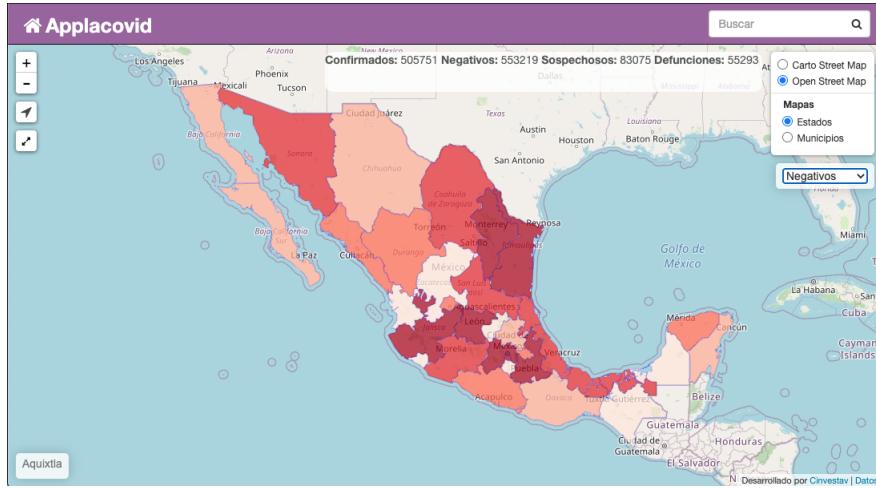


Figura 1.4: Capa de casos negativos por covid



Figura 1.5: Capa de casos sospechosos por covid

Al seleccionar la opción de “defunciones”, se despliega una capa de información de casos de defunciones con un rango de colores grises, donde la intensidad más clara indica un número menor casos, y por el contrario, una intensidad mayor indica un número alto de casos de defunciones (veáse la Figura 1.6).

Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte “sig.pdf”.

1.3.3. Subsistema: Consola de Administración

La es una aplicación web para administrar los subsistemas que componen Applacovid. Por medio de esta aplicación se puede: configurar la página web; generar códigos COVID-19 válidos para utilizarse en las aplicaciones móviles iOS y Android; y la más interesante, permitir a las autoridades de salud reportar cualquier caso positivo de COVID-19 ante Applacovid.



Figura 1.6: Capa de casos de defunciones por covid

Cuando un usuario se realiza una prueba de COVID-19 en alguno de los módulos autorizados por la secretaría de salud, por ejemplo, el Cinvestav, los médicos encargados y autorizados de realizar dicha prueba, pueden preguntar al usuario si desea reportarse ante Applacovid en caso de ser positivo con COVID-19. El usuario puede o no dar su consentimiento. En caso de dar su consentimiento, el usuario debe generar el código QR, por medio de la aplicación móvil Applacovid, para que el médico lo escaneé y pueda registrarla en la .

Una vez obtenido el resultado de la prueba, el personal médico autorizado debe reportar al usuario como positivo ante Applacovid por medio de la . El usuario podrá saber que ha dado positivo en la prueba cuando la aplicación móvil muestre el estado “Prueba positiva” en la pantalla principal de la aplicación. La interactúa con el *backend* de Applacovid para registrar a los usuarios con prueba positiva COVID-19. De esta manera, el personal médico autorizado puede registrar casos positivos ante Applacovid manteniendo segura la información del usuario.

Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte “ConsolaAdm.pdf”.

1.3.4. Subsistema: Aplicaciones móviles

Applacovid consiste de tres modos de funcionamiento principal: Protocolo de comunicación entre dispositivos, reporte de usuario con COVID-19 y notificación de riesgo de contacto. A continuación se describe cada uno de ellos.

Protocolo de comunicación entre dispositivos

Cuando Applacovid se instala en el dispositivo móvil se genera una llave de seguridad llamada *Kd*. Esta llave se utiliza para generar un identificador distinto cada 15 minutos titulado “identificador efímero” (*efID*). Este identificador efímero es generado a partir de procesos criptográficos que permiten ocultar la identidad del usuario. Una vez que la aplicación comienza a generar los identificadores efímeros, estos se transmiten hacia otros dispositivos móviles cercanos que tengan Applacovid instalada. Los *efID* se

transmiten vía Bluetooth entre los dispositivos y se envían junto con los saludos del protocolo Bluetooth. Este proceso se ilustra en la Figura 1.7.

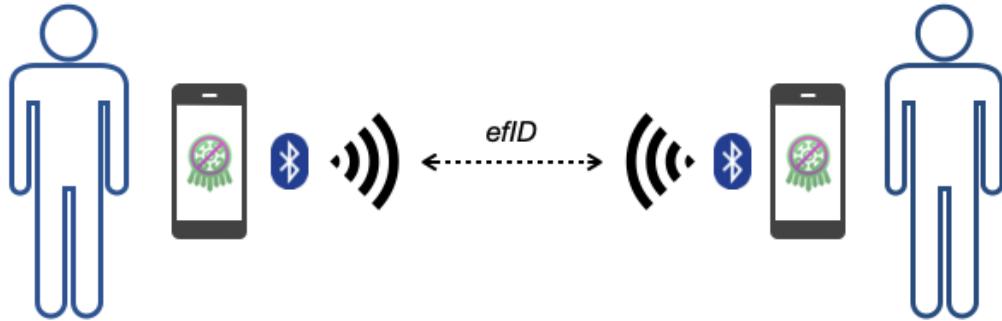


Figura 1.7: Detección de contactos vía Bluetooth.

Cuando un dispositivo recibe un saludo, vía Bluetooth, y en éste viaja el *efID*, se almacena localmente el ID recibido, el *timestamp* y la duración del encuentro. En las siguientes subsecciones se explican brevemente los fundamentos teóricos y conceptuales aquí descritos.

Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte “appmovil.pdf”.

Reporte de usuario con COVID-19

Cuando el usuario ha sido notificado positivo con COVID-19, puede reportarse de manera anónima ante Applacovid. Para ello, el usuario debe ingresar un código de seguridad, proporcionado por alguna autoridad de salud. Este código es único e intransferible. Los datos que viajan al servidor de Applacovid no contienen información personal del usuario, pero permite que otros usuarios, con la aplicación instalada, puedan ser alertados de un posible contagio, en caso de haber tenido contacto con el contagiado. El sistema garantiza la integridad y anonimato de los datos transmitidos y de la identidad real del contagiado COVID-19, respectivamente.

Notificación de riesgo de contacto

Cada **dos horas** Applacovid solicita una actualización de información al servidor. El servidor responde a estas solicitudes difundiendo la lista de identificadores efímeros, enviados por los usuarios que se reportaron con COVID-19.

Una vez recibida esta lista, cada uno de los dispositivos deriva los identificadores de los usuarios contagiados y los compara con los que tiene en su lista local. En caso de coincidencia, y si el nivel de riesgo es alto, se emite una notificación al usuario.

Creación de Identificadores Efímeros

Partiendo de una llave secreta K_0 , generada aleatoriamente, se genera una llave secreta para cada día d como sigue:

$$K_d = H(K_{d-1}),$$

donde H denota una función picadillo criptográfica segura.

La seguridad y anonimato del usuario es prioritario en esta aplicación, por lo tanto el identificador cambia cada **24 horas**, dando lugar a los identificadores efímeros ($efID$), los cuales serán utilizados en el *broadcast* (o saludos) que transmite el dispositivo, vía Bluetooth.

Cada día se utiliza la correspondiente llave secreta K_d , para generar todos los $efID$ que se usarán durante ese día de la siguiente forma:

$$efID_1, efID_2, \dots, efID_n = PRG(PRF(K_d, "sal")),$$

donde PRF es una función pseudo aleatoria usando el código de autenticación de mensajes (MAC), mientras que PRG es un generador pseudo aleatorio implementado por un cifrador por bloques en modo contador. La cadena “*sal*” es un parámetro del sistema que todos los usuarios conocen.

Cálculo del riesgo de infección

Cuando un usuario se reporta positivo con COVID-19 ante Applacovid, los dispositivos que tuvieron contacto con él tienen almacenado los $efID$, la distancia y la duración del encuentro. Con base en esta información, y tomando en cuenta la opinión de los expertos del sistema de salud, se genera un algoritmo para determinar si el usuario ha sido contagiado o no. El algoritmo es el siguiente:

1. Contacto lejano y de poca duración, es decir, dos personas sólo se cruzaron caminando sin tener una interacción directa.
2. Contacto lejano y de larga duración, dos personas dentro del rango de comunicación Bluetooth pero que no tienen interacción directa.
3. Contacto cercano de larga duración, podría representar a dos personas teniendo una conversación. O bien dos personas que caminaron durante cierto tiempo manteniendo proximidad, por ejemplo, un transbordo en el metro.

Recordando que hay medidas como la sana distancia, que establece un rango de metro y medio entre personas para reducir la probabilidad de contagio, y con base a la información disponible en los dispositivos, se puede ponderar un umbral para lanzar o no una notificación de posible contagio.

1.4. Productos esperados: Entregables

En esta sección se describen brevemente los entregables de acuerdo a lo especificado en el Anexo 2 del convenio del proyecto. Para detalles más específicos, se le solicita atentamente a los revisores que sean tan amables de consultar cada uno de los reportes técnicos generados para cada producto, tal y como se detalla a continuación.

1. **Aplicación Móvil.** Se desarrolló una aplicación móvil la cual puede ser descargada utilizando el paquete de distribución Android APK, el cual está disponible en el portal Internet del proyecto. También se cuenta con una biblioteca similar que utiliza la herramienta Xcode para dispositivos Apple que utilizan el sistema operativo iOS. Las pruebas de trabajo realizadas en la aplicación móvil indican su correcto funcionamiento en un rango muy amplio de teléfonos inteligentes desde gama baja/media a gama alta. Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte “appmovil.pdf”.

Asimismo, los manuales técnicos y del usuario de la versión Android y la versión iOS de Applacovid, pueden consultarse en los documentos "ios.pdf" y "android.pdf".

2. **Página Web.** Se diseñó y desarrolló un portal Internet, el cual contiene información relevante sobre Applacovid, y en el que se proporcionan diversos servicios relacionados con el tema de la pandemia COVID-19, tales como despliegue geográfico de zonas de riesgo basadas en estadísticas proporcionadas por el INEGI, boletines noticiosos, videos ilustrativos de la herramienta Applacovid, etc. Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte "pagina_web.pdf". Adicionalmente, el sistema de información geográfico web (SIGWeb) fue diseñado como una parte integral de la página web del proyecto Applacovid. Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte "sig.pdf".
3. **Procesamiento y base de datos.** Se generó toda la programación necesaria para el funcionamiento del servidor del sistema. El servidor del sistema se encarga de procesar la información enviada por un usuario que se reporta como contagio de covid y autentica la veracidad del contagio con la dependencia que certificó dicho contagio. También se encarga de recolectar las llaves secretas de los contagios diarios y de responder las solicitudes de los usuarios del envío de dicha información a sus dispositivos móviles. Los detalles técnicos, de concepto, diseño e implementación de este módulo son descritos profusamente en el documento adjunto a este reporte "ConsolaAdm.pdf".
4. **Documentación.** Además del presente reporte técnico, se produjo una manual técnico y manual del usuario de cada uno de los componentes principales de Applacovid. Asimismo, los manuales técnicos y del usuario de la versión Android y la versión iOS de Applacovid, pueden consultarse en los documentos "appmovil.pdf", "ios.pdf" y "android.pdf". Adicionalmente, se generaron tres videos ilustrativos de la aplicación, cuyos detalles pueden consultarse en el documento adjunto "videos.pdf".

1.5. Resultados

En esta sección se presentan los resultados científicos, académicos y de generación de recursos humanos obtenidos en el proyecto CONACyT 313572 : "Sistema descentralizado para detectar zonas de riesgo y contacto con personas confirmadas con COVID-19 protegiendo la privacidad de los participantes". La sección finaliza con una breve descripción de los problemas surgidos durante la ejecución del mismo y la manera en que dichos problemas fueron solucionados.

1.5.1. Resultados obtenidos

Se obtuvieron los siguientes resultados cualitativos y cuantitativos:

0. **Generación de conocimiento.** Los principales productos de investigación de este proyecto pueden ser resumidos así:
 - Tres artículos publicados en revistas JCR [6, 7, 4], de los cuales, uno de ellos fue publicado en la revista más importante por factor de impacto de las ciencias de la computación: *Communications of the ACM* [6]. La temática de los tres artículos estuvo relacionado con el tema de seguridad informática y criptografía. En particular, los pagos de derecho de publicación del artículo [7], fueron sufragados utilizando recursos del presupuesto del presente proyecto.

1. Resultados académicos

- Una tesis de maestría finalizada [8]. El tema principal de esta tesis de maestría fue el de aplicar tecnologías de *Blockchain* y computación en la nube, a un sistema de denuncias anónimas.
- Dos tesis de doctorado en proceso. El tema principal de la primera tesis de doctorado (a cargo del maestro en ciencias José Abraham Bernal Gutiérrez), gira alrededor del diseño e implementación eficiente de mecanismos criptográficos ligeros en dispositivos móviles con escasos recursos, así como en dispositivos de hardware reconfigurable FPGAs [1]. El tema principal de la segunda tesis de doctorado (a cargo del maestro en ciencias Jorge Emmanuel Chávez Saab), es el desarrollo de una función de retraso verificable ("Verifiable Delay Function" VDF por sus siglas en inglés) con resistencia a ataques cuánticos [3]. Las VDFs son consideradas un bloque fundamental para pruebas de trabajo y pruebas de posesión/participación para mineros trabajando en las *Blockchains* de cripto-monedas.³
- Una tesis de maestría en proceso. El tema principal de esta tesis de maestría (a cargo de la ingeniera Karla Jocelyn Campos Cruz), es la de investigar la seguridad asociada a la tecnología de balizas móviles [2].⁴

2. Desarrollos tecnológicos

Como se describió brevemente en §1.4, se desarrollaron las siguientes herramientas informáticas:

- Aplicación móvil para el rastreo de contactos Applacovid
- Portal Internet del sistema. Adicionalmente, el sistema de información geográfico web (SIG-Web) fue diseñado como una parte integral de la página web del proyecto Applacovid.
- Procesamiento y base de datos. Se generó toda la programación necesaria para el funcionamiento del servidor del sistema.

3. Difusión

Durante los seis meses de duración de este proyecto, y a partir de junio del presente año, se ofrecieron una serie de entrevistas, infografías y videos demostrativos de Applacovid, las cuales se enlistan a continuación.

- a) Video realizado para Camara de Diputados: "Jueves de Ciencia, Tecnología e Innovación"
<https://tinyurl.com/Applacovid-Diputados>
- b) Video de investigación en Primera Persona de Conexión Cinvestav
<https://tinyurl.com/Applacovid-Conexion-Video>
- c) Postcad: "Contact Tracing App para México", Estornuda.me, Ciencia y COVID-19
<https://tinyurl.com/Applacovid-Estornudame>
- d) Animatic de la solución abierta de Applacovid
<https://tinyurl.com/Applacovid-Animatic>
- e) Video informativo de la solución abierta de Applacovid
<https://tinyurl.com/Applacovid-abierta>
- f) Video informativo de la solución cerrada de Applacovid
<https://tinyurl.com/Applacovid-cerrada>
- g) Infografía "App que avisa de posible contagio"
(véase apéndice A)

³ "Proof of Work" (PoW) y "Proof of Stake" (PoS) en inglés.

⁴ "Beacons BLE" por sus siglas en inglés.

- h) Entrevista con el canal 22: "LIMINAL, la ciencia en movimiento"
<https://tinyurl.com/Applacovid-Canal22>
- i) Boletín de prensa de Conexión Cinvestav: "Planean desarrollar app para notificar la posibilidad de contagio por covid-19"
<https://tinyurl.com/Applacovid-BoletinE1>
4. Solicitamos y obtuvimos contacto formal a través de entrevistas vía video conferencia con las siguientes entidades gubernamentales:
- **Dra. Claudia Sheinbaum, Jefa de Gobierno de la CDMX y con la oficina del Gobierno Digital de la Agencia Digital de Innovación Pública de la CDMX.** Sostuvimos una breve video reunión con la Dra. Sheinbaum, y tres reuniones de trabajo con la Agencia Digital de Innovación Pública de la CDMX. Desafortunadamente, no logramos llegar a un punto de acuerdo en el despliegue de nuestra herramienta digital.
 - **Dirección General del CONACyT.** A través de las gentiles atenciones de la doctora Delia Aideé Orozco Hernández, obtuvimos una carta de apoyo firmada por la Dra. María Elena Álvarez-Buylla Roces, la cual estaba dirigida a Google y Apple. En dicha carta, la Dra. Álvarez-Buylla nos avala como desarrolladores nacionales de aplicaciones de rastreo de contagiados COVID-19.
 - **Secretaría de Salud.** A pesar de nuestros múltiples intentos de contacto con la Secretaría de Salud, todos nuestros esfuerzos fueron infructuosos.
 - **Infotec, Centro de Investigación e Innovación en TIC.** Contactamos al Dr. Feliú D. Sagols Troncoso, con quien sostuvimos discusiones enriquecedoras de cómo poder establecer colaboraciones entre nuestros dos grupos de investigación
 - **Centro de investigación en Computación del IPN.** Sostuvimos discusiones enriquecedoras de cómo poder establecer colaboraciones entre nuestros dos grupos
 - **Cinvestav.** Hemos planificado reuniones de trabajo con diversos grupos de investigación del Cinvestav que se encuentran empeñados en desarrollar pruebas rápidas de COVID-19 en las sedes de zacatenco, Monterrey e Irapuato.

1.5.2. Perspectivas de desarrollo hacia el futuro

Applacovid funciona utilizando tecnología Bluetooth (se mantiene como opción tecnológica el utilizar conexión inalámbrica del tipo WiFi). Para este proyecto fue fundamental garantizar el correcto funcionamiento del Bluetooth entre la mayoría de los dispositivos que son utilizados por toda la población mexicana. Por lo anterior fueron adquiridos teléfonos inteligentes de distintos rangos de precios y fabricantes, ya que dependiendo del fabricante, las características de los componentes pueden tener mucha variabilidad. De esta manera, fue posible hacer pruebas de la aplicación y garantizar su correcto funcionamiento para un espectro amplio de dichos dispositivos.

Nos gustaría resaltar de que dentro del Departamento de Computación del Cinvestav-IPN, hay grupos de investigación que realizan proyectos en el área de cómputo móvil. Estos proyectos, suelen requerir el uso de teléfonos móviles. Sus temas de investigación incluyen el desarrollo de aplicaciones móviles, así como estudios específicos de consumo energético y de ejecución de algoritmos de seguridad en plataformas específicas de cómputo móvil. Es así como estamos ciertos de que una vez terminado el presente proyecto, los teléfonos inteligentes adquiridos serán muy útiles para otros trabajos de investigación desarrollados al seno del Departamento. Ello fomentará la formación de recursos humanos en el área de cómputo móvil de nuestros programas de maestría y doctorado.

Los proyectos que se han realizado en computo móvil pueden ser verificados en la lista de graduados del Departamento de Computación, en el siguiente portal Internet: https://www.cs.cinvestav.mx/lista_graduados.html. A manera de ilustración, señalamos la tesis: "Soporte multi-plataforma de espacios colaborativos ejecutables en arreglos de dispositivos móviles", desarrollada el año 2016.

1.6. Problemas surgidos y solución de los mismos

A continuación se detallan los siguientes problemas técnicos y logísticos más importantes hallados durante el desarrollo de este proyecto.

- **Falta de interés y colaboración con las autoridades de la Secretaría de Salud.** No obstante nuestros mejores deseos de establecer un contacto formal con las autoridades de la Secretaría de Salud Federal, todos nuestros esfuerzos fueron infructuosos. Muy a nuestro pesar, debemos señalar de que ninguno de los múltiples correos electrónicos, y otros medios de contacto enviados a la sección epidemiológica de la Secretaría de Salud, fueron atendidos.
- **Postura de los gigantes informáticos Google y Apple.** Por primera vez en su corta historia, los gigantes informáticos Google y Apple forjaron una alianza para el desarrollo conjunto de una infraestructura básica para rastreo de contactos utilizando la tecnología Bluetooth presente en todos sus teléfonos celulares inteligentes. Como "dueños" del hardware, estas compañías informáticas tienen la capacidad de establecer políticas de uso que son muy difíciles de detener, incluso para gobiernos de países o federaciones de países con mucho poderío económico, como los Estados Unidos, o la Comunidad Europea. Posteriormente, Google y Apple ampliaron sus proyecciones iniciales, y decidieron desarrollar un aplicación móvil de rastreo con características muy semejantes a Applacovid. Más aún, tanto Google como Apple establecieron políticas muy restrictivas para aceptar en sus tiendas de aplicaciones *PlayStore* y *Appstore*, respectivamente, aplicaciones móviles creadas por terceros que tengan funcionalidad de rastreo vía Bluetooth.
Considerando lo explicado anteriormente, estimamos que en la actualidad el mercado de oportunidad más prometedor de Applacovid, sería en la protección de comunidades cerradas y con una comunidad de usuarios moderada tales como campi universitarios, empresas, dependencias gubernamentales, escuelas y colegios, etc.
- **Dificultades para ejercer el presupuesto.** Debido al muy peculiar contexto que padecemos debido a la pandemia mundial de COVID-19, experimentamos una enorme dificultad para ejercer el presupuesto solicitado al CONACyT para este proyecto. Por ejemplo, nos fue imposible ejercer la partida asignada de viáticos, pues las estancias técnicas de equipos de trabajo están suspendidas hasta nuevo aviso en el Cinvestav (véase §1.6.1 para más detalles en este punto).

1.6.1. Ajustes en el presupuesto

Con respecto al ajuste en equipo de cómputo, cabe mencionar de que esta acción se suscitó debido a que inicialmente se presupuestó la adquisición de dos servidores. Al analizar nuestras necesidades con nuestro equipo de desarrollo se optó por modificar nuestras adquisiciones. Fue así como se compró un servidor de alto rendimiento capaz de procesar cientos de solicitudes por segundo y albergar el sistema informático requerido por Applacovid. Se adquirieron además, dos computadoras de escritorio que fueron muy útiles para el desarrollo de la aplicación y la administración de los sistemas. Además se habilitaron otras dos computadoras pertenecientes al laboratorio de cómputo, con las cuales se hicieron experimentos e implementaciones utilizando los dispositivos FPGA y microcontroladores adquiridos también mediante

este proyecto. Adicionalmente, se adquirieron tres fuentes ininterrumpibles de energía (conocidas como nobreaks) y un proyector para trabajo de desarrollo colaborativo y reuniones de trabajo.

En el rubro de actividades, publicaciones y materiales, el tiempo tan acotado para la realización de este proyecto, nos impidió recibir de manera oportuna, las revisiones por pares en revistas científicas. Debido a ello, no pudimos ejercer parte del presupuesto asignado a este rubro. La única publicación pagada con el presupuesto del proyecto fue [7].

En dicha publicación se presentaron resultados de implementaciones en FPGAs que hicimos de diversos algoritmos de criptografía ligera, los cuales podrían ser utilizados para enriquecer la seguridad que actualmente presta la aplicación desarrollada, ya que es idónea para ser implementada en dispositivos restringidos como los teléfonos inteligentes con Bluetooth. Además, se trabajó en la evaluación de algunos algoritmos de criptografía ligera en los microcontroladores adquiridos.

Otro rubro no utilizado fue el de arrendamiento de activo fijo el cual fue solicitado para adquirir servicios de cómputo en la nube con el fin de hacer pruebas finales de los servicios de nuestra aplicación móvil del lado del servidor, contemplando un cómputo muy intensivo y una gran cantidad de usuarios. Sin embargo, gracias a la adecuada selección de nuestro servidor de cómputo, no consideramos necesarias dichas pruebas en la nube ya que con la infraestructura adquirida con nuestro servidor de alto rendimiento, hemos podido realizarlas localmente.

Durante el transcurso del proyecto solicitamos un cambio de rubro hacia la partida de equipo de laboratorio, con el fin de adquirir balizas bluetooth⁵, las cuales nos permitirían realizar pruebas de estrés a la aplicación móvil nativa en Android e Iphone, simulando más de cien dispositivos bluetooth interactuando con la misma. Lamentablemente, debido al súbito cierre presupuestal en nuestra institución de acuerdo a un comunicado recibido de la Secretaría de Hacienda, nos fue imposible ejercer ese recurso.

De esa manera, la simulación y pruebas de estrés se tuvieron que realizar mediante el apoyo de estudiantes, amistades y familiares, quienes instalaron la aplicación Android en sus celulares y reportaron fallas que fueron resueltas por el equipo de desarrollo. Se alcanzó la cifra de 97 usuarios con una amplia diversidad de teléfonos inteligentes y distintas versiones de sistema operativo Android.

Cabe señalar que a pesar de las dificultades arriba señaladas, consideramos que los ajustes solicitados no afectaron negativamente los resultados y entregables señalados en el Convenio de Asignación de Recursos.

⁵Conocidas en inglés como *beacons BLE*.

Bibliografía

- [1] José Abraham Bernal Gutiérrez, Protocolo de tesis de doctorado: “Diseño e implementación de mecanismos de seguridad en dispositivos restringidos” *Departamento de computación del Cinvestav*, 12 de mayo de 2018.
- [2] Karla Jocelyn Campos Cruz, Protocolo de tesis de maestría: “Análisis de las vulnerabilidades y contramedidas de seguridad para aplicaciones del internet de las cosas basadas en balizas Bluetooth” *Departamento de computación del Cinvestav*, 5 de Noviembre del 2020. Primera revisión.
- [3] Jorge Emmanuel Chávez Saab, Protocolo de tesis de doctorado: “Quantum Security Estimates for NIST Post-Quantum Protocols” *Departamento de computación del Cinvestav*, 20 de Noviembre de 2019.
- [4] Jesús-Javier Chi-Domínguez and Francisco Rodríguez-Henríquez, “Optimal strategies for CSIDH” *To appear in: Advances in Mathematics of Communications* [Volume and pages to be assigned] Disponible en:<https://www.aimsciences.org/article/doi/10.3934/amc.2020116>
- [5] INEGI, “En México hay 80.6 millones de usuarios de Internet y 86.5 millones de usuarios de teléfonos celulares”, *Comunicado de prensa Núm. 103/20*, 17 de febrero de 2020. Disponible en:<https://tinyurl.com/INEGI2020>.
- [6] Marcos Kiwi, Yoshiharu Kohayakawa, Sergio Rajsbaum, Francisco Rodríguez-Henríquez, Jayme Luiz Szwarcfiter, Alfredo Viola: A perspective on theoretical computer science in Latin America. *Communications of the ACM* 63(11): 102-107 (2020) Disponible en:<https://dl.acm.org/doi/10.1145/3419975>
- [7] Brisbane Ovilla-Martínez, Cuauhtemoc Mancillas-López, Alfredo Martínez-Herrera, José Abraham Bernal-Gutiérrez, “FPGA Implementation of Some Second Round NIST Lightweight Cryptography Candidates” *Electronics* Vol. 9, No. 11, paper 1940, 2020. Disponible en:<https://www.mdpi.com/2079-9292/9/11/1940>
- [8] Ángel Isaac Rodríguez Cosme, Tesis de maestría: “Arquitectura para un sistema de denuncias basado en Blockchain y tecnologías en la nube” *Departamento de computación del Cinvestav*, 24 de Noviembre del 2020. Disponible en:<https://www.mdpi.com/2079-9292/9/11/1940>

APÉNDICE A

Documentos relacionados

A.1. Infografía: “App que avisa de posible contagio”

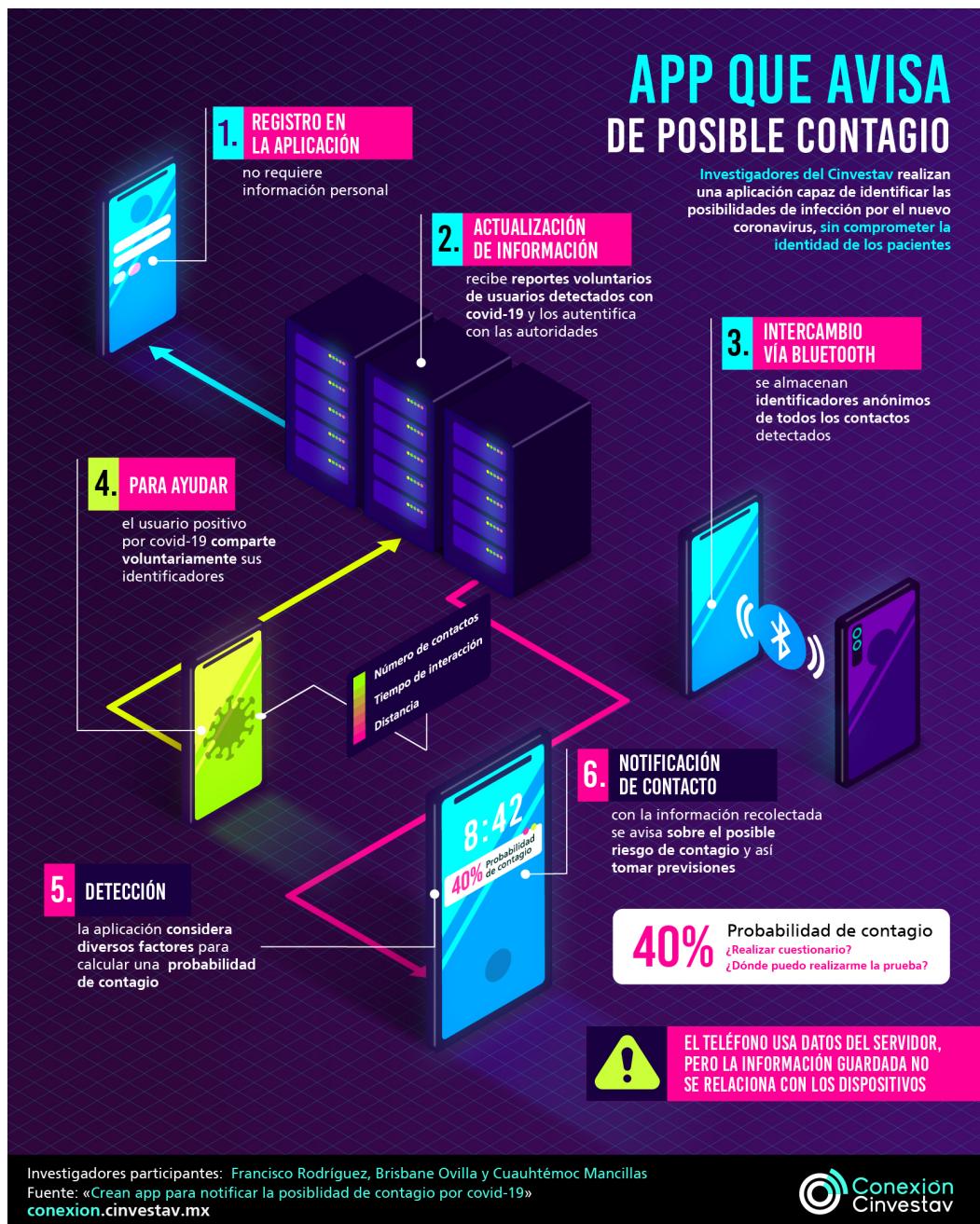


Figura A.1: Infografía: “App que avisa de posible contagio”.

A.2. Carta de apoyo Dra. Álvarez-Buylla dirigida a Google y Apple



GOBIERNO DE
MÉXICO

CONACYT
Consejo Nacional de Ciencia y Tecnología

2020
LEONA VICARIO
Méjico Comunicación de la ciencia

Mexico City, July 17, 2020

A0000/259/2020

Apple Inc. & Google LLC
Privacy-Preserving Contact Tracing Initiative.

Dear Sir/Madam,

In my capacity as Managing Director of Mexico's National Council of Science and Technology, I hereby endorse the CINVESTAV-IPN research group led by Dr. Cuauhtemoc Mancillas-López, Brisbane Martinez-Ovila and Francisco Rodríguez Henríquez, as one of the scientific groups authorized to develop the Mexican privacy-preserving COVID-19 contact tracing app. It is expected that this app will be massively deployed by millions of smart-phone users across Mexico.

The Mexican government is fully committed to strictly comply with Mexican data protection and privacy laws for its citizens, along with related regulations already in place.

Henceforth, I hereby support the Exposure Notification Entitlement Request to be submitted by the aforementioned research group in order to have full access to the Apple Inc. and Google LLD Exposure Notification Framework API.

Sincerely yours,

Maria Elena Álvarez-Buylla Roces, Ph.D.
Managing Director

Figura A.2: Carta de apoyo Dra. Álvarez-Buylla dirigida a Google y Apple