

**2-1000-2020-002205**

Bogotá D.C., 12 de Junio de 2020

Doctora

Amparo Yaneth Calderón Perdomo

Secretaria Comisión Primera

Congreso de la República

debatescomisionprimera@camara.gov.co

Ciudad

**Asunto:** Respuesta cuestionario CoronApp Aditiva 2

Respetada Señora Secretaria,

En atención a la comunicación mediante la cual se remitió la adición N° 2, para el debate de Control político a realizarse el próximo 16 de junio del año en curso, nos permitimos dar respuesta, de acuerdo con las competencias del Instituto Nacional de Salud.

**Manejo de datos personales y funcionamiento de CoronApp (MinTic, AND, Consejero para Innovación y la Transformación Digital, INS y Superintendente de Industria y Comercio)**

1. **¿Quién adaptó la aplicación existente en el país desde 2017, bajo qué modalidad de contrato y con qué costo?**

**Respuesta:**

La Agencia Nacional Digital, entidad pública adscrita al Ministerio de Tecnologías de la Información y las Comunicaciones fue la entidad encargada de adelantar las adaptaciones en el desarrollo, gestión, y mejoramiento continuo de la aplicación móvil CoronApp desde el mes de marzo de 2020. Esta adaptación se hizo a partir de una herramienta digital que tenía el INS previamente, la cual permitía hacer seguimiento a las condiciones de salud de los asistentes al evento masivo que implicó la visita del Papa a Colombia.

Esto proceso se hizo en el marco del memorando de entendimiento suscrito el día 6 de marzo del año en curso, entre el Instituto Nacional de Salud y la mencionada entidad. Dentro del mismo se estableció que la cooperación se encuentra orientada a apoyar estrategias implementadas por el Gobierno Nacional para la contención y mitigación de la pandemia del COVID-19 a través de medios digitales.

El costo del desarrollo es \$540.318.794, el costo de la implementación es \$83.124.358 y el costo de mantenimiento es de \$152.384.186, para un total de \$775.827.338.

2. **¿Quién está llevando a cabo la auditoría del código fuente?**

**Respuesta:**

Se está llevando a cabo un proceso con la firma externa Price wáter house coopers quien hace un acompañamiento constante a la Agencia Nacional Digital mediante la evaluación de controles de seguridad de CoronApp, la cual consiste en realizar pruebas de seguridad a nivel de aplicación, backend e infraestructura. Una vez realizados estos controles se surte un proceso de retroalimentación mediante el cual la Agencia adopta medidas de seguridad que mitigan las posibles vulnerabilidades, todo ello con el objetivo de lograr las mejores prácticas en seguridad y de construcción del código.

**3. ¿Por qué el código fuente que fue público desde 2017, dejó de publicarse a partir de las adaptaciones de 2020?**

**Respuesta:**

El código fuente para mitigar y controlar brotes epidemiológicos contaba con una licencia GNU. Este año se iniciaron las modificaciones y ajustes necesarios al código fuente, siempre actualizándose a las diferentes etapas de la pandemia y a los nuevos requerimientos, de modo que se mantiene un constante ajuste del código para poder cumplir con las necesidades cambiantes.

Por ello dentro de la estrategia, está no liberar el código fuente pues se considera que el nivel de sensibilidad y reserva de la información que se maneja en la aplicación corre riesgos al publicarlos. Al no liberarlo, se evita la posibilidad de hacer ingeniería inversa, y con ello, que potenciales hackers entiendan cómo funciona el algoritmo.

Cabe precisar que cuando un código es de interés nacional, como es el caso de CoronApp, generalmente las regulaciones lo eximen de ser elegible para ser tratado como abierto, a fin de evitar el detrimento de la seguridad nacional, la vulneración de la confidencialidad de la información gubernamental, o que comprometa la razón de su creación al compartirlo.

En este sentido, al ser Coronapp la única aplicación móvil oficial del Gobierno Nacional que permite a los habitantes del territorio nacional, de manera gratuita (zera rating), tener acceso a información actualizada y veraz sobre emergencias sanitarias, su evolución en el país y alertas de prevención, así como reportar, a través de terminales móviles, un autodiagnóstico de su estado de salud, como lo indica el Decreto 614 del 30 de abril de 2020, y al ser parte de la estrategia institucional de respuesta sanitaria adoptada para enfrentar la pandemia del SARS CoV2, (resolución No. 779 del 19 de mayo de 2020 del Ministerio de Salud y Protección Social,) la información que se puede ver comprometida afecta directamente la salud, la seguridad nacional y la confidencialidad de los datos del usuario, valores amparados por la Ley 1712 de 2014.

Por último, la explicabilidad de algoritmos es una materia en desarrollo a nivel global y los entes internacionales recomiendan hacer público su funcionamiento, lo cual consta en los documentos de la Agencia Nacional Digital.

#### 4. ¿Por qué consideran que CoronApp está exenta de la aplicación de la ley de habeas data?

**Respuesta:**

En primer lugar, es importante aclarar que en ningún comunicado se ha manifestado que CoronApp está exenta de la aplicación de la Ley de Hábeas Data. Por el contrario, CoronApp cumple con los principios y requerimientos establecidos por la Ley 1581 de 2012 de protección de datos personales.

La información recolectada a través de CoronApp es tratada con estricto cumplimiento a las normas y protocolos de Hábeas Data, contemplando todas las medidas de protección y seguridad de la información, de acuerdo con los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad establecidos en la Ley 1581 de 2012 y en la “Política de tratamiento de información relacionada con CoronApp Colombia” cuyo enlace fue recientemente actualizado y puede ser consultada aquí: <https://www.ins.gov.co/Normatividad/PolíticasInstitucionales/politica-detratamientode-informacion-coronapp-colombia.pdf>

Acto seguido, se presentan las excepciones que trata el artículo 10 de la Ley 1581 de 2012, puntualmente para el presente caso aplican:

- a) Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial; (...)
- c) Casos de urgencia médica o sanitaria; (...)

Adicionalmente, como bien lo dice la parte final del artículo 10 antes citado “Quien acceda a los datos personales sin que medie autorización previa deberá en todo caso cumplir con las disposiciones contenidas en la presente ley” (subrayado fuera de texto), por lo que CoronApp no se encuentra exenta de cumplir con la ley 1581 de 2012 antes citada.

Por último, y conforme lo establecido por la Corte Constitucional en Sentencia C-748-11, “la aplicación del precepto bajo análisis debe subordinarse a que la entidad administrativa receptora cumpla con las obligaciones de protección y garantía que se derivan del citado derecho fundamental, en especial la vigencia de los principios de finalidad, utilidad y circulación restringida”.

Para finalizar, CoronApp cumple con los requisitos de seguridad requeridos por entidades como el HIPAA (Ley de Portabilidad y Responsabilidad del Seguro de Salud), PCI DSS (Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago), SOC (Central de Seguridad Informática que previene, monitorea y controla la seguridad en las redes y en Internet); las directrices de ISO/IEC 27001, 27017, 27018 e ISO 9000.

#### 5. ¿Cuántas de las personas que han descargado la app la usan de manera efectiva?

**Respuesta:**

Con corte a 10 de junio de 2020, han descargado la App a través de Google Play Store (Android) y Apple

Store (iOS) 9.869.090 personas, de los cuales 5.753.275 son usuarios activos.

6. **¿Cuáles fueron las razones para pasar de Google y Apple a blue trace en el protocolo de bluetooth?**

**Respuesta:**

Permanente se evalúan las mejores tecnologías para ser implementadas en el desarrollo de la plataforma, se evaluó con el equipo técnico el uso de la funcionalidad desarrollada por dichos fabricantes, sin embargo, no se usó el sistema desarrollado por Google y Apple, ya que cuando surgió la necesidad de salir a producción con un componente de blue trace no se encontraba en el mercado disponible para el uso la tecnología de Google-Apple, por lo que se debió actuar con diligencia para prevenir y salvar vidas con la mayor prontitud, además del éxito que ha tenido esta tecnología en otros países.

La tecnología Apple-Google solo lleva disponible unos días para su uso en el mundo y CoronApp empezó su brindar una solución desde hace más de 2 meses. Sin embargo, la funcionalidad de identificar las cercanías entre personas mediante el Bluetooth ya se encuentra implementada en CoronApp y es una estrategia más que ayudará a romper las cadenas de contagio.

**Seguimiento epidemiológico (INS y Min Salud)**

1. **¿Cuál es la función de la App en el plan epidemiológico?**

**Respuesta:**

El objetivo de la CoronApp, es identificar pacientes categorizados como alertas que han manifestado por medio del autoreporte sintomatología y factores de riesgo compatibles con Covid 19. Esta información es entregada a las entidades territoriales con el fin de facilitar la identificación oportuna de casos potenciales en el territorio nacional.

Es una estrategia tecnológica de vigilancia digital que permite apoyar el proceso de respuesta en salud pública frente a la Emergencia por Covid 19. La CoronApp establece la frecuencia y distribución de síntomas autoreportados por los usuarios de la CoronApp, definiendo categorías de riesgo.

Realiza un seguimiento continuo y sistemático a través de un mecanismo de vigilancia participativa con el fin de presentar datos e información útil y oportuna para orientar estrategias de prevención y control en el marco de la pandemia por COVID 19.

El componente espacial de la App, muestra la distribución geográfica de las categorías de riesgo. Los Sistemas de Información Geográfica (SIG) al servicio de la salud, se constituyen en una herramienta útil para la población, contribuyendo a disminuir la incertidumbre asociada a esta emergencia internacional. La definición de las variables de la CoronApp se encuentra en concordancia con el Protocolo de vigilancia

epidemiológica del evento. Han sido definidas a partir del algoritmo de riesgo determinado para identificar casos de COVID 19. Para hacer el seguimiento epidemiológico requiere que los usuarios realicen voluntariamente su declaración de síntomas y la actualización de estos en caso de presentarlos.

**2. ¿Qué medidas de policía se desprenden de la aplicación CoronApp?**

**Respuesta:**

A la fecha no se han contemplado en las funcionalidades de CoronApp alguna que permita la realización de medidas policivas.

**3. ¿Se aplican las reglas de historia clínica a la CoronApp?**

**Respuesta:**

Es necesario aclarar que CoronApp no se trata de una herramienta de telemedicina o asistencia médica virtual, el formulario de CoronApp no corresponde a un registro administrativo que tenga las características básicas de una historia clínica de que trata la Resolución número 1995 de 1999.

**4. ¿Cómo están aplicando las recomendaciones de la OCDE y la OMS en lo referente al seguimiento epidemiológico mediante herramientas tecnológicas?**

**Respuesta:**

Los datos recolectados por la Aplicación son de uso del Instituto Nacional de Salud con fines de mitigación de los efectos de la pandemia en el país, exclusivamente. CoronApp utiliza diferentes medidas técnicas y procedimientos de seguridad de la información, tendientes a garantizar la integridad, disponibilidad y confidencialidad de todos los datos personales suministrados en CoronApp (incluyendo datos sensibles y de menores de edad). Así mismo, evita su adulteración, pérdida, consulta, uso, acceso o divulgación no autorizada o fraudulenta. Para garantizar la seguridad de la información y protección de los datos personales registrados, se cuenta con protocolos y controles tales como:

- Políticas y procedimientos de protección de datos personales y seguridad de la información
- Controles administrativos, estratégicos, tácticos y tecnológicos en seguridad para el almacenamiento y tratamiento de la información.
- Acceso restringido a la aplicación y a la infraestructura.
- Implementación de buenas prácticas de seguridad para la administración y afinamiento de la infraestructura y desarrollo del código.
- Diferentes capas de seguridad a nivel de infraestructura.
- Software de seguridad perimetral.
- Desarrollo de pruebas de seguridad de manera constante, entre otros.

Además de las medidas mencionadas anteriormente para la protección de los datos, CoronApp Colombia cuenta con el apoyo y asesoría del Grupo de Respuesta a Emergencias Cibernéticas de Colombia – ColCERT-, para la prevención de amenazas tecnológicas, cibernéticas y aplicación de buenas prácticas y recomendaciones para el fortalecimiento de la seguridad y privacidad de la información.

CoronApp es una herramienta del Instituto Nacional de Salud – INS - para hacerle frente a la pandemia, por tanto, es la entidad que asume la responsabilidad sobre la seguridad de la información de la App.

Toda la información es anonimizada y está protegida, como se ha mencionado, se cuenta con estrictos protocolos y controles de protección de datos personales y seguridad de la información, controles administrativos, estratégicos, tácticos y tecnológicos en seguridad para el almacenamiento y tratamiento de la información, acceso restringido a la aplicación y a la infraestructura, diferentes capas de seguridad a nivel de infraestructura, software de seguridad perimetral y realización constante de pruebas de seguridad.

Respecto a con quién se comparten datos, tenemos que CoronApp da la opción que el usuario decida voluntariamente compartir cierta información, previa autorización expresa e informada, con su ARL, Aseguradora de salud y/o con su empleador, con las finalidades de que la(s) entidad(es) seleccionada(s) pueda(n):

- a. Gestionar los riesgos en los ambientes laborales y demás actividades económicamente productivas, en el marco del Sistema General de Riesgos Laborales, para proteger a la población trabajadora y sus familias de COVID-19.
- b. Gestionar la atención y prestación de servicios de salud en respuesta a posibles casos de enfermedad por el COVID-19.
- c. Dar aplicación a los protocolos, procedimientos y lineamientos definidos por el Ministerio de Salud y Protección Social y el Ministerio de Trabajo para la preparación, respuesta y atención de casos de enfermedad por el COVID-19, en el marco del Sistema de Gestión de la Seguridad y Salud en el Trabajo SG-SST.

El usuario puede seleccionar compartir su información con las tres entidades o solo con alguna de ellas o seleccionar “No autorizo compartir”. Estos permisos se pueden editar en cualquier momento a través de la sección “Permisos y privacidad” en el Menú de CoronApp, y cada vez que registre información se le consulta sobre esta autorización.

En caso que el usuario autorice compartir su información con alguna entidad, los datos que se comparten del usuario son (i) nombres y apellidos, (ii) tipo y número de documento, (iii) el nivel de riesgo (Normal, Advertencia o Alerta) según el autodiagnóstico reportado en CoronApp, y (iv) localización geográfica del usuario y el dispositivo al momento de realizar el reporte del autodiagnóstico en CoronApp. Esta opción está desactivada por defecto, solo se activa por autorización expresa del usuario, y cada vez que el haga un reporte.

Es de resaltar que la calidad del dato supone la buena fe de quien lo suministra pues la herramienta es tipo participativo voluntario y no una obligación impuesta. La comprobación de la calidad del dato se hace cuando la secretaria de salud se pone en contacto con el usuario de acuerdo con el nivel de riesgo.

El tiempo del tratamiento de los datos recolectados a través de CoronApp Colombia será el estrictamente

necesario para realizar las actividades que despliegue el Ministerio de Salud y Protección Social para la contención y mitigación del coronavirus COVID-19, así como para el análisis del comportamiento del virus que deban realizar las entidades de salud del país.

Por último, es pertinente aclarar que la información recolectada a través de CoronApp es tratada con estricto cumplimiento a las normas y protocolos de Hábeas Data, contemplando todas las medidas de protección y seguridad de la información, de acuerdo con los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad establecidos en la Ley 1581 de 2012 y en la “Política de tratamiento de información relacionada con CoronApp Colombia” cuyo enlace fue recientemente actualizado y puede ser consultada aquí:

<https://www.ins.gov.co/Normatividad/PolíticasInstitucionales/politica-detramientode-informacion-coronapp-colombia.pdf>

Cordialmente,



**MARTHA LUCIA OSPINA MARTINEZ**

Directora General

Indicar en letras el número de anexos y entre paréntesis su contenido y el número de folios

No. Anexos:

No. Folios:

Nombre  
anexos:

**Elaboró:** MAY BIBIANA OSORIO MERCHAN

**Revisó:** LUIS ERNESTO FLOREZ SIMANCA