- **Procedimiento nº.: PS/00222/2021**

Recurso de reposición Nº RR/00189/2022

Examinado el recurso de reposición interpuesto por ***SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL*** (en lo sucesivo, la SEDIA) contra la resolución dictada por la Directora de la Agencia Española de Protección de Datos (en lo sucesivo, AEPD) en el procedimiento sancionador PS/00222/2021, y en base a los siguientes

HECHOS

PRIMERO: Con fecha 18 de febrero de 2022, se dictó resolución por la Directora de la AEPD en el procedimiento sancionador PS/00222/2021, en virtud de la cual se imponía la sanción de **APERCIBIMIENTO**, por la vulneración de lo dispuesto en los artículos:

- Artículos 5.1.a) y 5.2 del RGPD, tipificada en el artículo 83.5.a) del RGPD y en el artículo 72.1. a) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.

- Artículos 12 y 13 del RGPD, tipificada en el artículo 83.5.b) del RGPD y en el artículo 72.1.h) de la LOPDGDD, a los solos efectos de determinar los plazos de prescripción.

- Artículo 25 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado d), a los solos efectos de determinar los plazos de prescripción.

- Artículo 28.3 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado k), a los solos efectos de determinar los plazos de prescripción.

- Artículo 28.10 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado m), a los solos efectos de determinar los plazos de prescripción.

- Artículo 35 del RGPD, tipificada en el artículo 83.4.a) del RGPD y en el artículo 73 de la LOPDGDD en el apartado t), a los solos efectos de determinar los plazos de prescripción.

Dicha resolución, que fue notificada al recurrente en fecha 28 de febrero de 2021 a través de servicio de Soporte del Servicio de Notificaciones Electrónicas y Dirección Elec-

trónica Habilitada, fue dictada previa la tramitación del correspondiente procedimiento sancionador, de conformidad con lo dispuesto en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales (en adelante, LOPDGDD), y supletoriamente en la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas (en adelante, LPACAP), en materia de tramitación de procedimientos sancionadores.

SEGUNDO: Como hechos probados del citado procedimiento sancionador, PS/00222/2021, quedó constancia de los siguientes:

PRIMERO: El Real Decreto 403/2020, de 25 de febrero, desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital. Se publicó el 27 de febrero de 2020 en el BOE, entrando en vigor el mismo día de su publicación.

Dispone en su artículo 1 que el METD se encarga de

"la política de telecomunicaciones y para la transformación digital, en particular impulsando la digitalización de las Administraciones Públicas".

Dentro de este marco, la SEDIA tiene, conforme al artículo 8, atribuidas las funciones de

"el impulso de la digitalización del sector público y la coordinación y cooperación interministerial y con otras Administraciones Públicas respecto a dichas materias, sin perjuicio de las competencias atribuidas a otros departamentos ministeriales".

La SGAD, conforme al artículo 9, es:

"el órgano directivo al que corresponde, bajo la autoridad de la persona titular de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la dirección, coordinación y ejecución de las competencias atribuidas al Departamento en materia de transformación digital de la administración, incluyendo el desarrollo técnico y aplicación de las Leyes 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas, y 40/2015, de 1 de octubre, y su normativa reglamentaria, en lo que concierne a la actuación y funcionamiento del sector público por medios electrónicos."

SEGUNDO: El Real Decreto 454/2020, de 10 de marzo, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales fue publicado en el BOE de 12 de marzo de 2020. Entró en vigor el mismo día de su publicación en el BOE hasta el 6 de agosto de 2020, fecha en la que entró en vigor el Real Decreto 735/2020 de 4 de agosto.

En su artículo 1 dispone:

Corresponde al Ministerio de Sanidad, la propuesta y ejecución de la política del Gobierno en materia de salud, de planificación y asistencia sanitaria, así como el ejercicio de las competencias de la Administración General del Estado para asegurar a los ciudadanos el derecho a la protección de la salud.

En su artículo 3 dispone:

1. La Dirección General de Salud Pública, Calidad e Innovación es el órgano que asume las funciones relativas a la sanidad exterior; la promoción de la salud y la prevención de las enfermedades y lesiones; la coordinación de la vigilancia en salud pública; (…).

2. Le corresponde la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica, el impulso de planes de salud y programas de calidad en el Sistema Nacional de Salud, incluido el Plan Nacional sobre el SIDA, así como el análisis y evaluación del funcionamiento del sistema sanitario español y su comparación con otros sistemas sanitarios. (…)".

TERCERO: El Real Decreto 463/2020, de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, en el artículo 4.2.d) designa al Ministro de Sanidad como autoridad competente delegada en su área de responsabilidad.

CUARTO: Con fecha 28 de marzo de 2020 se publica en el BOE la Orden SND/297/2020, de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

El resuelvo primero dice:

Primero. Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

1. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo urgente y operación de una aplicación informática para el apoyo en la gestión de la crisis sanitaria ocasionada por el COVID-19. Dicha aplicación permitirá, al menos, realizar al usuario la autoevaluación en base a los síntomas médicos que comunique, acerca de la probabilidad de que esté infectado por el COVID-19, ofrecer información al usuario sobre el COVID-19 y proporcionar al usuario consejos prácticos y recomendaciones de acciones a seguir según la evaluación.

La aplicación permitirá la geolocalización del usuario a los solos efectos de verificar que se encuentra en la comunidad autónoma en que declara estar. La aplicación puede incluir dentro de sus contenidos enlaces con portales gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

La aplicación no constituirá, en ningún caso, un servicio de diagnóstico médico, de atención de urgencias o de prescripción de tratamientos farmacológicos. La utilización de la aplicación no sustituirá en ningún caso la consulta con un profesional médico debidamente cualificado.

El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular de la aplicación será la Secretaría General de Administración Digital. El Ministerio de Sanidad, como responsable del tratamiento, autoriza a la Secretaría General de Administración Digital a recurrir a otros encargados en la

ejecución de lo previsto en este apartado.

2. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de un asistente conversacional/chatbot para ser utilizado vía whatsapp y otras aplicaciones de mensajería instantánea. Proporcionará información oficial ante las preguntas de la ciudadanía. El diseño estará basado en información oficial del Ministerio de Sanidad.

El responsable del tratamiento será el Ministerio de Sanidad y el encargado del tratamiento y titular del chatbot será la Secretaría de Estado de Digitalización e Inteligencia Artificial a través de la Subdirección General de Inteligencia Artificial y Tecnologías Habilitadoras Digitales.

3. Encomendar a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de una web informativa con los recursos tecnológicos disponibles.

Se constata que la aplicación Radar COVID no está incluida dentro de las soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios dada su finalidad, que es distinta: la trazabilidad de los contactos.

Su finalidad se extrae, entre otros, de:

-La "Información general" facilitada por el Gobierno de España cuando indica: ¿Qué es Radar COVID?:

https://radarcovid.gob.es/faq-informacion-general

Radar COVID es una aplicación móvil desarrollada para ayudar a controlar la propagación de la COVID-19 a través de la identificación de los posibles contactos estrechos de casos confirmados a través de la tecnología Bluetooth.

Del "EXPONEN" Séptimo de la Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID, que dice:

Séptimo.

Que «Radar COVID» es una aplicación para dispositivos móviles que promueve la salud pública mediante un sistema de alerta de contagios por la COVID-19. La aplicación, mediante el empleo de identificadores aleatorios efímeros que no guardan relación con la identidad del teléfono móvil empleado o el usuario, detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación descargada y activa, El dispositivo de cada usuario descarga periódicamente las claves Bluetooth de todos los usuarios de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias competentes), procediendo a determinar si el usuario ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a evitar que el virus se propague.

QUINTO: En el mes de abril de 2021 se celebra una reunión que tiene por objeto abordar el "Diseño, desarrollo, piloto y evaluación de un sistema que permita

la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Intervienen las siguientes personas:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
A.A.A.	*SEDIA*
B.B.B.	*SEDIA*
C.C.C.	*SEDIA*
D.D.D.	*SEDIA*
E.E.E.	*Mº Sanidad*
F.F.F.	*Mº Sanidad*
G.G.G.	*SEDIA*
H.H.H.	*Gobierno de Canarias*
I.I.I.	*Minsait*
J.J.J.	*Minsait*
L.L.L.	*Minsait*
M.M.M.	*Minsait*
N.N.N.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*

Los asuntos tratados son:

Se presenta el documento anexo 20200721_Seguimiento SEDIA v5 dónde se recoge el resumen ejecutivo de las conclusiones del análisis de resultados del piloto.

El acuerdo adoptado es:

Se acuerda tener listo para el próximo martes día 28/07/2020 el listado de acciones a llevar cabo sobre la app de cara a una puesta en producción inminente, ya sea en una CCAA, ciudad o a nivel nacional. Se acuerda también preparar un documento descriptivo con un resumen del funcionamiento de la app para que las diferentes CCAA puedan analizar su funcionamiento.

SEXTO: Con fecha 6 de mayo de 2020 el METD publica la siguiente nota de prensa:

"España trabaja a nivel nacional y europeo para la interoperabilidad de las aplicaciones de prevención de contagios frente al COVID-19.

La vicepresidenta tercera del Gobierno y ministra de Asuntos Económicos y Transformación Digital, Nadia Calviño, junto a los secretarios de Estado de Digitalización e Inteligencia Artificial, Carme Artigas, y de Telecomunicaciones e Infraestructuras Digitales, O.O.O., participaron en este encuentro para buscar una posición europea común que permita aprovechar las posibilidades que ofrece la tecnología para contribuir a la gestión de la pandemia y a la posterior recuperación a nivel europeo.

Entre dichas soluciones digitales se puso el foco en las aplicaciones de prevención de contagios. En ese sentido, España destacó la importancia de encontrar

un enfoque coordinado a nivel europeo para estas aplicaciones que garantice la interoperabilidad y permita realizar una salida conjunta de la emergencia sanitaria. Además, se señaló la necesidad de aprovechar el potencial que ofrece la economía digital para contribuir a la gestión de la pandemia, siendo necesario encontrar un equilibrio entre los beneficios derivados de estas innovaciones y la privacidad, la seguridad y las cuestiones éticas. (…)

La secretaria de Estado de Digitalización e Inteligencia Artificial, Carme Artigas, compartió con las autonomías la posición de España a nivel europeo, así como los avances que prepara la Comisión Europea sobre estas herramientas digitales. El objetivo es aunar esfuerzos y compartir puntos de vista sobre las posibilidades existentes en torno al desarrollo de estas aplicaciones y su interoperabilidad, buscando respuestas coordinadas en base a las necesidades de los diferentes territorios".

SÉPTIMO: Con fecha 9 de junio de 2020 la Directora General de Salud Pública, Calidad e Innovación del MSND envió una carta al Secretario General de Administración Digital (SGAD) con el siguiente tenor:

"En relación a la prueba piloto de la aplicación móvil para la trazabilidad de contactos del COVID-19 que está previsto llevar a cabo en la Comunidad Autónoma Canarias, le comunico el visto bueno de este Ministerio para su desarrollo.

Para la realización de la misma, a nuestro juicio, debería remitirse a la Agencia Española de Protección de Datos toda la información que corresponda para garantizar el cumplimiento de la normativa vigente en esta materia.

Por otro lado, entendemos que el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la comunidad en que se va a llevar a cabo.

Agradeciendo el trabajo que está realizando la Secretaría de Estado de Digitalización e Inteligencia Artificial en la respuesta frente al COVID-19, reciba un cordial saludo."

OCTAVO: Con fecha 11 de junio de 2020 entra en vigor el, ya derogado, Real Decreto-ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Los artículos 5, 26 y 27, disponían:

Artículo 5. Planes y estrategias de actuación para afrontar emergencias sanitarias.
Con arreglo a lo previsto por el artículo 65 de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, se procederá a la adopción de planes y estrategias de actuación para afrontar emergencias sanitarias, mediante actuaciones coordinadas en salud pública, atendiendo a los distintos niveles de riesgo de exposición y de transmisión comunitaria de la enfermedad COVID-19 para el desarrollo de las distintas actividades contempladas en este real decreto-ley.

Artículo 26. Provisión de información esencial para la trazabilidad de contactos. Los establecimientos, medios de transporte o cualquier otro lugar, centro o entidad pública o privada en los que las autoridades sanitarias identifiquen la necesidad de realizar trazabilidad de contactos, tendrán la obligación de facilitar a las autoridades sanitarias la información de la que dispongan o que les sea solicitada relativa a la identificación y datos de contacto de las personas potencialmente afectadas.

Artículo 27. Protección de datos de carácter personal.

"1. El tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y aplicación del presente real decreto-ley se hará de acuerdo a lo dispuesto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, y en lo establecido en los artículos ocho.1 y veintitrés de la Ley 14/1986, de 25 de abril, General de Sanidad. En particular, las obligaciones de información a los interesados relativas a los datos obtenidos por los sujetos incluidos en el ámbito de aplicación del presente real decreto-ley se ajustarán a lo dispuesto en el artículo 14 del Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta las excepciones y obligaciones previstas en su apartado 5.

2. El tratamiento tendrá por finalidad el seguimiento y vigilancia epidemiológica del COVID-19 para prevenir y evitar situaciones excepcionales de especial gravedad, atendiendo a razones de interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016. Los datos recabados serán utilizados exclusivamente con esta finalidad.

3. Los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias, que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

4. El intercambio de datos con otros países se regirá por el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, teniendo en cuenta la Decisión n.º 1082/2013/UE del Parlamento Europeo y del Consejo, de 22 de octubre de 2013, sobre las amenazas transfronterizas graves para la salud y el Reglamento Sanitario Internacional (2005) revisado, adoptado por la 58.ª Asamblea Mundial de la Salud celebrada en Ginebra el 23 de mayo de 2005."

Se constata que este real decreto ley no habilita para el desarrollo la aplicación Radar COVID.

NOVENO: Con fecha 15 de junio de 2020 se acordó por el Secretario General de la Administración Digital la contratación de los servicios para la trazabilidad de contactos con relación a la pandemia ocasionada por la COVID 19 a Indra Tecnologías de la Información S.L.

Según consta en el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, apartado 1 bajo el epígrafe "Antecedentes":

La Orden SND/297/2020, de 27 de marzo, del Ministro de Sanidad encargó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

En particular, dicha Orden establece en su resolución primera, el Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

Adicionalmente, la Dirección General de Salud Pública, Calidad e Innovación, de la Secretaría General de Sanidad (Ministerio de Sanidad) ha dado el Visto Bueno a una prueba piloto de rastreo de contactos en relación a la COVID-19, encargando a la SEDIA el desarrollo de una aplicación móvil para tal fin.

Según consta en el objeto del contrato el proyecto de implantación tendría tres fases: fase pre-piloto, fase piloto y fase post-piloto.

El "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19", aceptado por INDRA, recoge en el objeto del contrato las necesidades a cubrir y entre otras, las siguientes cláusulas:

"5.4. Infraestructura en la nube (cloud).

Se precisará que los desarrollos del Backend se realicen en una infraestructura en la nube en modo de autogestión, para facilitar la agilidad en el desarrollo de la solución.

No obstante, lo anterior, tanto el almacenamiento como cualquier actividad de tratamiento de datos se ubicarán en el territorio de la Unión Europea, ya sean éstos provistos y gestionados por la empresa adjudicataria o por sus contratistas y colaboradores, y se alojarán en servidores y/o centros de proceso de datos de la propia empresa adjudicataria o de sus contratistas.

…

En la medida de lo posible, se procurará la utilización de componentes en la infraestructura cloud que permitan la migración futura de la solución a la nube SARA de la AGE.

6.1. Confidencialidad en general

El contratista se compromete a garantizar la más estricta confidencialidad y reserva sobre cualquier dato o información a los que pueda tener acceso o pudiera conocer con ocasión de la ejecución del contrato, así como sobre los resultados obtenidos de su tratamiento, y a que únicamente se utilizarán para la consecu-

ción del objeto del contrato, no pudiendo comunicarlos, utilizarlos, ni cederlos a terceros bajo ningún concepto, ni siquiera para su conservación. Estas obligaciones se extienden a todas las personas que, bajo la dependencia del contratista o por su cuenta, hayan podido intervenir en cualquiera de las fases de ejecución del contrato.

La obligación de confidencialidad y reserva conlleva la de custodia e impedir el acceso a la información y documentación facilitadas y a las que resulten de su tratamiento de cualquier tercero ajeno al servicio contratado, entendiéndose como tal tanto cualquier persona ajena a la empresa contratista como cualquiera que, aun no siéndolo, no esté autorizada para acceder a tal información.

Asimismo, el contratista se compromete a velar por la integridad de los datos, es decir, a la protección de la información facilitada y a la que resulte de su tratamiento contra la modificación o destrucción no autorizada de los datos.

6.2. Protección de datos personales

Se deberá cumplir lo estipulado en la ley orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales, adaptada al Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, y por el que se deroga la Directiva 95/46/CE(Reglamento General de Protección de Datos), incluyendo lo dispuesto en la disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre y en el Real Decreto 3/2010, de 8 de enero.

Conforme a la Disposición adicional primera de la Ley Orgánica 3/2018, de 5 de diciembre, de Medidas de seguridad en el ámbito del sector público, las medidas de seguridad a aplicar en el marco de los tratamientos de datos personales se corresponderán con las de la Administración púbica de origen y se ajustarán al Esquema Nacional de Seguridad.

Se requerirá a INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU la manifestación expresa del sometimiento a la normativa nacional y de la Unión Europea en materia de protección de datos conforme a los artículos 35.1d y 122.2 de la LCSP modificado por artículo 5 del Real Decreto Ley 14/2019, de 31 de octubre, por el que se adoptan medidas urgentes por razones de seguridad pública en materia de administración digital, contratación del sector público y telecomunicaciones.

6.3. Seguridad

INDRA SOLUCIONES TECNOLOGÍAS DE LA INFORMACIÓN, SLU implementará las medidas técnicas y organizativas de seguridad apropiadas y elaborará la documentación pertinente, de acuerdo con el correspondiente análisis de riesgos, según lo establecido en el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración electrónica.

7 PROPIEDAD INTELECTUAL

Sin perjuicio de lo dispuesto en la legislación vigente en materia de propiedad intelectual, el adjudicatario acepta expresamente que la propiedad de todos los productos que sean elaborados por el adjudicatario, incluidos sus empleados y en su caso cualquier empresa subcontratada, en ejecución del Contrato y, en particular, todos los derechos de propiedad intelectual y/o industrial que deriven

de los mismos, corresponde únicamente a la administración contratante, con exclusividad y sin más limitaciones que las que vengan impuestas por el ordenamiento jurídico.

A los efectos previstos en el párrafo anterior, la empresa adjudicataria se compromete a la entrega a la SGAD de toda la documentación técnica, trabajos y materiales generados, en cuyo poder quedarán a la finalización del Contrato sin que el contratista pueda conservarla, ni obtener copia de esta, ni utilizarla o facilitarla a terceros sin la expresa autorización de la SGAD, que la daría, en su caso, previa petición formal del contratista con expresión del fin."

También recoge en el ANEXO I las características del sistema aplicación móvil y el elemento backend en infraestructura pública:

ANEXO I. CARACTERÍSTICAS DEL SISTEMA APLICACIÓN MÓVIL

1. Inicio y bienvenida aplicación: aviso legal, onboarding informativo, activación de seguimiento Bluetooth. Uso de SDK Google/Apple anónimo y redirección a repositorio genérico (Backend).

a. Permite al usuario la transmisión y recepción de identificadores aleatorios a través del Bluetooth

b. Verificación del código de autorización por parte de la autoridad sanitaria ante positivo por COVID-19. De cara al piloto, como es previsible que no se disponga del servicio de la autoridad sanitaria se simulará la validación del positivo que desencadene el proceso de tracing y se pueda pilotar.

c. Envía al servidor su baliza generadora de claves efímeras en caso de positivo.

d. Pantallas estáticas informativas.

e. Interacción con el SDK google/apple, de acuerdo a la funcionalidad proporcionada:

i. Gestionar las claves aleatorias diarias:

1. Generar diariamente las claves de exposición temporales y rotar los identificadores efímeros basados en ellos.

2. Proveer las claves al Backend para usuarios diagnosticados, incluyendo los valores temporales.

3. Acepta las claves de la App para la detección de exposición, incluyendo las fechas y los niveles de riesgo de transmisión.

4. Almacena claves en el dispositivo.

ii. Gestionar el envío y escaneo Bluetooth:

1. Gestión del envío de claves.

2. Escanea claves emitidas por otros dispositivos.

3. Almacenar las claves observadas en un almacenamiento en el dispositivo.

4. Identificar cuando otro usuario en contacto ha sido un caso confirmado.

5. Calcular y proveer el riesgo de exposición a la aplicación.

6. Presentar las siguientes peticiones de permiso al usuario:

a. Antes de empezar a escanear y enviar las claves.

b. Antes de proveer al servidor las claves al servidor central tras haber sido contagiado.

2. Comunicación de casos positivos:

a. Introducción QR/código COVID-19 (manual, escáner o importación) personal y de uso único.

b. Aviso confirmación QR validado positivo: pantalla informativa.

c. Cuestionario opcional (en caso de positivo): recoge datos anónimos básicos para su tratamiento Backend App (código postal, sintomatología y su fecha, patologías previas,…).

3. Notificación de riesgo: aviso de contacto con positivo confirmado y pantalla de recomendaciones.

4. Salida de la aplicación: posibilidad de salida de la aplicación en cualquier momento, eliminando cualquier rastro de claves efímeras utilizadas.

ELEMENTO BACKEND EN INFRAESTRUCTURA PÚBLICA

1. Gestión de datos en Backend

a. Servir información necesaria para funcionamiento de la App (si se estima necesario. Alternativamente la App puede ser autocontenida).

b. Validación con el sistema de autorización sanitaria ante diagnósticos positivos (si este sistema no estuviera disponible se realizaría una Simulación de esta validación). La aplicación debe comunicarse con un servidor externo (sanitario) que provea el código de autorización que confirme el positivo y pueda autorizar a subir las balizas al servicio en función del siguiente ciclo propuesto:

i. Sistema médico solicita token/QR autenticación al Backend para confirmar positivo COVID-19.

ii. Paciente recibe token/QR autenticación para confirmar el positivo COVID-19.

iii. Paciente envía el token/QR autorizado al Backend para subir su histórico de contactos.

Como es previsible que no se disponga del servicio de la autoridad sanitaria en el alcance inicial se simulará la validación del positivo que desencadene el proceso de tracing para que se pueda probar su funcionamiento.

c. Base de datos con servicio de información centralizada que permita el rastreo de contactos y la gestión de balizas.

i. Recolectar las balizas de los usuarios que hayan sido diagnosticados de COVID-19.

ii. Distribuir las balizas de los casos confirmados hacia los dispositivos.

iii. Integración servicio de autorización de positivos.

iv. Integración con sistemas Terceros. Estudio de la interoperabilidad con Backends de otros Estados para asegurar funcionalidad transfronteriza.

2. Seguridad

a. Implantación de controles para prevenir ataques específicos a nivel de aplicación.

b. Securización comunicaciones con otros dispositivos y con sistemas sanitarios.

c. Anonimización de señales entre dispositivos.

3. Simulación: capacidad de emular respuesta COVID-19 positivo, a efectos de testing (testear comportamiento de tracing).

DÉCIMO: La SEDIA ha acreditado los siguientes certificados emitidos a favor de INDRA:

o *ISO 27018 Certificado de Privacidad en la Nube: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de emisión del certificado.*

o *ISO 27001 Certificado del Sistema de Gestión de Seguridad de la Información: Los sistemas de información que soportan los procesos de negocio y activos de información necesarios para la prestación de servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según la declaración de aplicabilidad en vigor a fecha de realización de la auditoría.*

o *STI-0014/2009 Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información: El SGS de los servicios de outsourcing de TI Administración, Soporte, Explotación e Infraestructura), tanto en entornos físicos como virtualizados cloud), según el catálogo de servicios en vigor. Certificado del Sistema de Gestión de Servicio de Tecnologías de la Información.Para la gestión del sistema RADAR COVID, INDRA ha contratado los servicios de Amazón Web Services INC.*

*UNDÉCIMO: Con fecha 17 de junio de 2020 se celebra una reunión del grupo de trabajo interterritorial al que asisten representantes de las Comunidades Autónomas de Andalucía, Aragón, Asturias, Castilla y León, Extremadura, Galicia, Islas Baleares, Islas Canarias, La Rioja, Madrid, Murcia, Navarra y Valencia y de la ciudad autónoma de Melilla, así como por parte de la Secretaría de Estado de Digitalización e Inteligencia Artificial asisten **D.D.D.**, Subdirector General de Impulso de la Digitalización de la Administración, **C.C.C.**, asesor técnico para el desarrollo de la aplicación, el equipo técnico a cargo de desarrollo de la aplicación y **P.P.P.**, asesora Gabinete.*

Se expone que:

"…tres principales objetivos de la aplicación: preservar la salud pública, ir un paso por delante de la COVID-19 y minimizar su impacto económico facilitando el movimiento de las personas. Para ello, hay tres momentos clave a tener en cuenta: la activación del Bluetooth (que permite preservar la anonimidad de los usuarios), el reporte de diagnósticos positivos y la notificación a usuarios en riesgo de contagios.

(…)

También se destaca la importancia de la privacidad para la aplicación, garantizando en todo momento la anonimicidad de las personas, permitiendo que la app pueda desactivarse en cualquier momento, almacenando los datos de forma descentralizada solo durante 14 días o generando los avisos en la propia app.

Por último, se explica cómo se comporta técnicamente la aplicación: los teléfonos intercambian identificadores Bluetooth aleatorios y, con el consentimiento del usuario, el teléfono carga el histórico de los últimos 14 días de claves en el servidor. Cada teléfono descarga periódicamente las claves Bluetooth de todas las personas diagnosticadas que lo han reportado y que han podido estar en contacto. Con ello, se envían las notificaciones de alerta de contagios."

DUODÉCIMO: Consta un documento denominado "Diseño Piloto Covid-19 App. Presentación CCAA 17 junio 2020, elaborado por la SEDIA.

En este se definen los parámetros clave del Piloto:

a) Duración

- *15 días de APP activa*
- *Fecha de inicio tentativa: Semana del 29 de Junio.*

b) Ubicación:

- *San Sebastián de La Gomera (7.921 habitantes, INE datos provisionales 1/01/2020), municipio ubicado en la Isla de La Gomera.*

c) Participantes:

- *Residentes en el municipio captados por distintos canales de acceso al piloto.*
- *Turistas residentes en Tenerife que simulen movimiento por el municipio durante el piloto.*

d) Alcance de Piloto: Volumen de participantes

- *Se potenciará la mayor participación posible combinando distintos canales de acceso a la misma, estimándose un volumen entre 2.000 y 3.000 usuarios de la APP .*
- *Se establecerá aproximadamente un 10% de casos con Positivo en COVID simulado inicial, para favorecer la detección de casos de riesgo y así comprobar funcionamiento de APP.*

e) Valoración cumplimiento objetivos

- *Análisis datos cuantitativos*
- *Análisis cualitativo: encuestas anónimas y tests de usuarios en remoto (15 usuarios).*

También recoge los "Canales de acceso al Piloto" por los participantes:

Se proponen 4 canales de acceso a la APP para participación controlada en el piloto, a confirmar con el gobierno de Canarias y gobierno local de La Gomera

1. Comunicación directa individual a Empleados públicos

Personas que residen en San Sebastián de la Gomera y trabajan como empleados públicos en distintos ámbitos y personas que residen en Tenerife y puedan desplazarse como "turistas simulados" al municipio durante el piloto

2. Agentes Instaladores

Equipo de agentes que promoverán y ayudarán en la descarga de la APP en espacios públicos y oficinas de atención al ciudadano del municipio, potenciando la captación de personas jóvenes y mayores de 65 años

3. Teléfono de información específico

Posibilidad de habilitar un teléfono para facilitar el acceso a aquellos ciudadanos del municipio que estén interesados en participar, así como para posible comprobación simulada de contagios

4. Buzoneo postal

Valorar la posibilidad de cartas directas o folletos depositados en buzón físico a todos los residentes en el municipio que explique el piloto e invite a participar

DÉCIMO TERCERO: Consta, con fecha 23 de junio de 2020, una nota de prensa publicada por el METD, con el siguiente tenor:

"El Gobierno aprueba el desarrollo del piloto para una aplicación móvil de notificación de contactos de riesgo por COVID-19. (…)

El objetivo es que el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y en coordinación con el Servicio Canario de la Salud, ponga en marcha la próxima semana una prueba piloto de esta herramienta tecnológica en la isla canaria de La Gomera.

El piloto tiene como objetivo evaluar aspectos técnicos y de experiencia de uso del ciudadano, con el fin de optimizar el diseño de la aplicación y su grado de confianza. También servirá para calibrar el algoritmo de la app con el fin de garantizar la veracidad de las notificaciones. (…)

Una vez concluida y evaluada la prueba piloto en un escenario real, se podrán tomar las decisiones oportunas para la conexión con el sistema de salud de las diferentes comunidades autónomas.

Esta herramienta tecnológica se suma a las medidas ya puestas en marcha por las autoridades sanitarias para seguir los contactos de los contagios de COVID-

19 y que, junto a las medidas de prevención adoptadas, están contribuyendo al control de la pandemia. El contrato aprobado en Consejo Ministros por el procedimiento de emergencia se ha suscrito con la empresa Indra Soluciones Tecnológicas de la Información S.L.U. por un importe de 330.537,52 euros, IVA incluido. (…)

Privacidad

El desarrollo utiliza un modelo descentralizado, basado en el protocolo Decentralized Privacy-Preserving Proximity Tracing (DP-3T), el más respetuoso con la privacidad del usuario. Esto implica que sólo se envían al servidor los identificadores cifrados que cada móvil emite, no los que recibe de otros terminales cercanos. Cada cierto tiempo los móviles descargan los nuevos identificadores de contagios confirmados para comparar con sus registros. Es decir, que el cotejo de datos y análisis de riesgo se lleva a cabo siempre en el móvil del usuario y no en un servidor, lo que garantiza la privacidad.

Esta aplicación cumple, por tanto, con todas las garantías fijadas por la normativa europea para salvaguardar la intimidad de la ciudadanía. Además, garantiza la proporcionalidad y minimiza el uso de datos personales. El uso de la aplicación será voluntario y enmarcado en los límites de la emergencia sanitaria, en estricto cumplimiento de las recomendaciones de la Comisión Europea al respecto."

DÉCIMO CUARTO: Consta, con fecha 23 de junio de 2020, en la Referencia del Consejo de Ministros, el siguiente Acuerdo:

"ACUERDO por el que se toma razón de la declaración de emergencia para la contratación de los servicios de diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación a la pandemia ocasionada por la COVID-19, con una duración de 5 meses, por un importe de 330.537,52 euros, IVA incluido."

"APROBADO EL DESARROLLO DEL PILOTO PARA UNA APLICACIÓN MÓVIL DE NOTIFICACIÓN DE CONTACTOS DE RIESGO POR COVID-19.

El Consejo de Ministros ha dado luz verde al contrato para diseñar, desarrollar y evaluar una prueba piloto para una aplicación móvil que permita notificar a los contactos de un usuario el posible riesgo de contagio por COVID-19. El objetivo es que el Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, y en coordinación con el Servicio Canario de la Salud, ponga en marcha la próxima semana una prueba piloto de esta herramienta tecnológica en la isla canaria de La Gomera. El piloto tiene como objetivo evaluar aspectos técnicos y de experiencia de uso del ciudadano, con el fin de optimizar el diseño de la aplicación y su grado de confianza. También servirá para calibrar el algoritmo de la app con el fin de garantizar la veracidad de las notificaciones. Una vez concluida y evaluada la prueba piloto en un escenario real, se podrán tomar las decisiones oportunas para la conexión con el sistema de salud de las diferentes comunidades autónomas. Esta herramienta tecnológica se suma a las medidas ya puestas en marcha por las autoridades sanitarias para seguir los contactos de los contagios de

COVID-19 y que, junto a las medidas de prevención adoptadas, están contribuyendo al control de la pandemia. El contrato aprobado en Consejo Ministros por el procedimiento de emergencia se ha suscrito con la empresa Indra Soluciones Tecnológicas de la Información S.L.U. por un importe de 330.537,52 euros, IVA incluido."

DÉCIMO QUINTO: Con fecha 29 de junio de 2020 se lanza por el Gobierno de España el proyecto piloto que se extiende hasta el 31 de julio de 2020 en la isla de La Gomera.

En el documento de seguimiento de fecha 24.07.2020, constan las siguientes fases y fechas sobre la planificación del piloto Radar COVID:

Consta publicado un Informe de conclusiones (https://radar-resources.s3-eu-west-1.amazonaws.com/28-01-2020-InformeRadarCOVID.pdf) elaborado por la SEDIA, fechado el 28 de enero de 2021, que indica:

La app permite

• Verificar el código de autorización por parte de la autoridad sanitaria ante positivo por COVID-19

• Permite al usuario la transmisión y recepción de identificadores aleatorios a través del Bluetooth

• Envía al servidor su baliza generadora de claves efímeras en caso de positivo

• Pide al servidor las claves anónimas de usuarios contagiados de manera periódica

• Mostrar notificaciones al usuario con instrucciones de qué hacer en caso de que haya estado en contacto a otro usuario positivo COVID-19

Su desarrollo está soportado sobre la alianza Google & Apple para la implementación de un API común encargado de gestionar y proporcionar a los dispositivos claves aleatorias anónimas y su intercambio vía bluetooth a través de las siguientes funciones:

Gestionar las claves aleatorias diarias

• Generar diariamente las claves de exposición temporales y rotar los ids efímeros basados en ellos

• Provee las claves a la aplicación para usuario diagnosticados, incluyendo los valores temporales

• Acepta las claves de la app para la detección de exposición, incluyendo las fe-

chas y los niveles de riesgo de transmisión

• Almacena claves en el dispositivo

Gestiona el envío y escaneo Bluetooth

• Gestión el envío de claves

• Escanea claves emitidas por otros dispositivos

• Almacena las claves observadas en un almacenamiento en el dispositivo

• Identifica cuando otro usuario en contacto ha sido un caso confirmado

• Cálculo y provee el riesgo de exposición a la aplicación

• Presenta las siguientes peticiones de permiso al usuario:

• Antes de empezar a escanear y enviar las claves

• Antes de proveer al servidor las claves al servidor central tras haber sido contagiado G

Objetivos y metodología del piloto

Duración:

• 15 días de APP activa (fases de monitorización y ampliación de monitorización)

• Fecha de inicio: Semana del 29 de junio (fase de comunicación y divulgación)

• Fecha de fin: semana del 20 de julio (fase de análisis de conclusiones)

Ubicación:

San Sebastián de La Gomera (aproximadamente 10.000 habitantes incluyendo residentes, turistas y personas que se desplazan diariamente por motivos de trabajo), municipio ubicado en la Isla de La Gomera.

Participantes

• Residentes en el municipio captados por distintos canales de acceso al piloto.

• Visitantes residentes en Tenerife que se desplazaron al municipio durante el piloto, captados por distintos canales de acceso al piloto.

Alcance de Piloto: Volumen de participantes

• Se potenciará la mayor participación posible combinando distintos canales de acceso a la misma, estimándose un volumen entre 2.000 y 3.000 usuarios de la APP

• Se establecerá aproximadamente un 10% de casos con Positivo en COVID simulado, para favorecer la detección de casos de riesgo y así comprobar funcionamiento de APP

Valoración cumplimiento objetivos

• Análisis datos cuantitativos

• Análisis cualitativo: encuestas anónimas y tests de usuarios en remoto (15 usuarios)

Objetivo del piloto

(…) Así, el objetivo del piloto fue monitorizar el funcionamiento de la APP de forma controlada para:

1. Optimizar el diseño de APP (…)

2. Comportamientos y preferencias en materia de prevención de los ciudadanos (…)

3. Contrastar hipótesis de partida (…)

4. Obtener insights para el despliegue (…)

Alcance

Como se ha mencionado anteriormente, el piloto se ha planteado desde una perspectiva simulada y controlada, de forma que permite obtener conclusiones de valor respecto a su funcionamiento, uso y comportamiento por parte de la ciudadanía, pero limita la obtención de datos en relación a algunos aspectos:

Descarga abierta vs descarga controlada

Si bien en un primer momento se planteó la posibilidad de controlar el acceso a la descarga de la aplicación exclusivamente al público objetivo del piloto, residentes, trabajadores o visitantes de San Sebastián de la Gomera, se decidió finalmente dejarla abierta debido a 3 factores clave:

• Complejidad de implementación.

• Impacto negativo en la usabilidad por parte de los ciudadanos al tener que introducir códigos de acceso para la descarga.

• Incorporar un factor ajeno al propio funcionamiento de la aplicación en el supuesto despliegue nacional.

Privacidad vs información cualificada.

En el piloto se ha seguido la misma premisa que rige la propia aplicación, la garantía de protección de datos personales y el anonimato en el uso de Radar CO-

VID.

En esa línea, se ha recopilado información agregada de los usuarios de la aplicación, tanto de las personas que se la descargaban, como de las personas que asumían el papel de Casos positivos o recibían notificaciones de alerta de riesgo de contagio.

Esta información agregada impide obtener información comportamental o por perfiles más cualificados de ciudadanos, así como un análisis sociológico de propagación del virus.

Simulación vs Realidad

La estrategia del piloto se basó en una simulación de casos positivos por parte de voluntarios que introdujeron el código que les fue asignado, creando por tanto un brote de propagación ficticio y forzado que no permite analizar de (sic) propagación real de la enfermedad que sería monitorizada por la aplicación.

Metodología.

Enfoque del piloto.

• Conseguir el mayor número de usuarios posible, habilitando distintos canales de acceso a la participación por parte de los ciudadanos objetivo del piloto.

• Incorporar participantes de distintos perfiles poblacionales para detectar facilitadores y barreras de uso diferentes.

• Priorizar la comprobación de la funcionalidad y experiencia de uso de la APP simulando un volumen de casos de positivos elevado (10% de la estimación de población usuaria de la APP durante el piloto) que favoreciera la generación de los KPIs clave de evaluación del piloto, pero manteniendo una tasa de incidencia acumulada prevista razonable desde el punto de vista epidemiológico (2,2%).

• Mantener el control de los casos positivos e introducción de códigos en la APP, limitando el acceso solo a muestras controladas.

• Obtener feedback directo de usuarios del piloto que permita optimizar el diseño.

Monitorización y agilidad en toma de decisiones

Con el objetivo de disponer de información continua sobre evolución de los distintos indicadores de éxito del piloto y reorientar su enfoque si era necesario para alcanzar el objetivo final, se crearon distintas herramientas de reporte y control, que permitirían incorporar los datos recogidos de forma anónima y voluntaria:

• Plantilla diaria de registro de participantes captados por promotores, recogiendo información agregada de sexo y edad del conjunto de personas captadas en cada jornada de promoción.

• *Plantilla diaria de entrega de códigos positivos por promotores, recogiendo también información agregada de sexo y edad de las personas a las que se asignaba el papel de voluntario positivo.*

• *Plantilla diaria de registro de llamadas en CAU, según motivo de llamada*

• *Plantilla diaria de registro de contenido de llamadas por riesgo de alerta, para la que se creó un argumentario de llamada.*

• *Cuadro de mando global de indicadores clave de participantes, códigos, notificaciones y demás información que se especifica en el apartado de conclusiones.*

El seguimiento continuo de la información permitió tomar decisiones ágiles como el desplazamiento de los promotores a nuevas zonas ante posible saturación de las zonas iniciales o la incorporación de nueva oleada de contagios en naviera.

Resultados del piloto Metodología de evaluación de la eficacia de Radar COVID

Las cuestiones relevantes para evaluar la eficacia de Radar COVID son:

Comportamiento del usuario y actitud hacia la aplicación, evaluando si éste ha favorecido el propósito de Radar COVID en función de:

Adopción ¿Está Radar COVID logrando suficiente masa crítica para ser eficaz? ¿Se adoptan las nuevas versiones de la app?

Compromiso y participación ¿Está motivado el usuario y cumple las instrucciones que facilitan la contención de la pandemia? ¿Es rápido en el cumplimiento de las instrucciones? ¿Cómo de positiva es la foto al contrastarla con iniciativas comparables en Europa?

Retención

Una vez instalada, ¿el usuario continúa con la aplicación activa y en uso o, por el contrario, pierde el interés y la desactiva? Desempeño de la aplicación en la detección del riesgo de contagio entre ciudadanos:

Simulación del brote ¿Cuántos contactos estrechos es capaz de detectar Radar COVID por cada caso positivo confirmado a través de la aplicación?

Resultados que permiten evaluar la eficacia de Radar COVID

Adopción

¿Se ha alcanzado un nivel de adopción que permita obtener conclusiones de funcionamiento y eficacia de Radar COVID?

El nivel de adopción conseguido durante el piloto ha permitido comprobar el funcionamiento de la aplicación y testar su eficacia ante casos positivos de COVID-19, si bien su resultado no es extrapolable al despliegue nacional al haber tenido un nivel promoción en el municipio muy elevado y dirigido.

A la finalización del piloto se habían conseguido más de 58.000 descargas totales, el 90% en Android, y solo en el periodo de activación directa en San Sebastián de la Gomera, entre los días 6 y 20 de julio, la cifra ronda las 11.000 descargas.

Por las limitaciones indicadas en el apartado anterior, no es factible diferenciar cuántas de estas descargas pertenecen a SS de La Gomera para confirmar la previsión objetivo de las 3.500 descargas aproximadamente en el municipio que representaría el 35% de adopción, si bien se pueden realizar algunas estimaciones que sí confirmarían haber alcanzado el umbral deseado, siendo conservadores en la previsión:

• Descargas "asistidas": 924. Descargas que han sido realizadas de forma fehaciente por los agentes promotores ubicados tanto en el municipio de SS de La Gomera como en los barcos colaboradores en el piloto.

• Empleados públicos: Se impulsó la participación de 758 empleados públicos de los 3 ámbitos institucionales (Ayuntamiento de SS de La Gomera, Cabildo de La Gomera y Servicios de Salud) y se les invitó a que promovieran también la descarga en su entorno más cercano.

• Si asumimos que la tasa de participación es similar a la tasa obtenida de introducción de códigos positivos (61%) y que cada empleado público lo compartió con una media de 3 personas de su entorno más próximo, obtenemos una participación promovida por este colectivo de unos 1.850 usuarios de la aplicación.

• Participación espontánea: Si consideramos que las campañas de difusión y promoción de la iniciativa realizadas a través de ruedas de prensa, notas informativas, actividad en redes sociales e información disponible en los aviones de la compañía BINTER, despertaran el interés de la población del municipio e impactara en una descarga voluntaria de al menos un 2% de la población, se habrían conseguido 200 descargas adicionales.

• Descargas web del Gobierno de Canarias: se han registrado 241 clics al enlace de descarga directa en la web; estimamos que todos los clics han materializado la descarga 66 Con estas estimaciones, se puede concluir que la cifra alcanzada de descarga se sitúa en 3.215 y por tanto ha permitido evaluar la eficacia y funcionamiento de Radar COVID, ya que la cifra final real estimamos que pueda situarse entre este umbral mínimo de 3.215 y las 11.675 descargas que se han producido durante la duración del piloto. Cabe destacar que la tasa de adopción es especialmente alta, considerando adicionalmente que, de los 10.000 habitantes de San Sebastián de La Gomera, aproximadamente un 10% de la población tiene una edad inferior a 10 años (edad límite inferior considerada para tener smartphone y un 11% son personas mayores de 75 años donde podría haber menor tasa de penetración de estos dispositivos, siguiendo la distribución de población publicada por el INE correspondiente a 1 de Enero de 2020 para el conjunto de la isla de La Gomera. Extrapolando al conjunto de la población nacional en el momento de despliegue global, será difícil conseguir esta tasa de adopción, si bien de cara al piloto ha permitido realizar los análisis necesarios del funcionamiento de la app.

DÉCIMO SEXTO: Consta un documento denominado "COVID Radar. Secretaría General de Administración Digital. Funcionamiento general. Madrid, Junio 2020" donde la SEDIA informa lo siguiente:

Estrategia de la app Covid-19

Objetivos de la app

• Preservar la salud pública sin renunciar a la privacidad de los ciudadanos

• Ir un paso por delante del Covid-19: alertar a personas en riesgo es contener el virus de forma proactiva

• Minimizar el impacto económico del Covid-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas

Los momentos clave

• Activación del Bluetooth

• Reporte de diagnósticos positivos

• Notificación a usuarios en riesgo de contagio

Foco en privacidad

La app cuenta con un proceso de gestión de datos con la privacidad por diseño, velando en todo momento por la anonimidad de los usuarios, según la normativa vigente y estándares europeos.

Las medidas de privacidad contempladas en la primera versión de la solución son las siguientes:

• No se requiere login, ni se solicita al usuario ningún dato personal sea identificativo o no

• El usuario puede desactivar la app cuando quiera

• Para registrar las interacciones entre dispositivos de forma anonimizada, se generan identificadores aleatorios cambiantes que preservan la identidad de los dispositivos

• El acceso a los datos de dichas interacciones se realiza únicamente cuando se diagnostica un nuevo positivo COVID-19 o cuando el Servicio Médico lo considera necesario

• Los datos se almacenan de forma descentralizada durante un plazo de 14 días, tras el cual son suprimidos

• Las notificaciones a usuarios expuestos al Covid-19 se generan en la propia app, sin requerir identificar el dispositivo o el número de teléfono del usuario

También contiene la "Descripción funcional de la app" y el "Funcionamiento de las alertas de contagio Bluetooth".

DÉCIMO SÉPTIMO: Consta un documento denominado "Radar COVID. Seguimiento: 17.07.2020", elaborado por la SEDIA junto al Servicio Canario de Salud, el Gobierno de Canarias, el Gobierno del Cabildo de La Gomera y el Ayuntamiento de San Sebastián de La Gomera donde se informa lo siguiente:

¿Qué observamos diariamente?

Comportamiento del ciudadano

Descargas Acumuladas Radar COVID: 54.591

- *Hay más de **54.000 descargas a nivel nacional**, el 94% en Android*
- *De las casi 10.000 descargas desde el inicio del piloto, nuestros **promotores** han confirmado **924 descargas**, más **59 en web***
- *Se ha impulsado la descarga entre **758 voluntarios** o empleados públicos*

Y respecto al Plan de Acción Fase 3- Semana 20 a 27 julio Análisis de datos y obtención de conclusiones, dice:

DÉCIMO OCTAVO: Con fecha 21 de julio de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Asisten:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
A.A.A.	*SEDIA*
B.B.B.	*SEDIA*
C.C.C.	*SEDIA*
D.D.D.	*SEDIA*
Q.Q.Q.	*Gobierno de Canarias*
R.R.R.	*SEDIA*
E.E.E.	*Mº Sanidad*
F.F.F.	*Mº Sanidad*

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
H.H.H.	*Gobierno de Canarias*
I.I.I.	*Minsait*
J.J.J.	*Minsait*
L.L.L.	*Minsait*
M.M.M.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*

Asuntos tratados:

Se presenta el documento anexo 20200717_Seguimiento SEDIA v13.PPTX dónde se recogen los avances en el piloto Radar COVID.

Acuerdos adoptados:

Se acuerda presentar en el próximo comité de seguimiento un informe completo con el análisis de las conclusiones que se ha extraído de la ejecución ya finalizada del piloto en la isla de La Gomera.

DÉCIMO NOVENO: Consta un documento denominado "Radar COVID. Seguimiento: 24.07.2020" elaborado por la SEDIA junto al Servicio Canario de Salud, el Gobierno de Canarias, el Gobierno del Cabildo de La Gomera y el Ayuntamiento de San Sebastián de La Gomera, donde se informa lo siguiente:

Escalada e integración con Servicios Sanitarios

Tras recopilar propuestas de las Comunidades Autónomas, nos decantamos por un esquema de generación de códigos centralizado y gestión descentralizada

Análisis de datos

Se han analizado los resultados del piloto en base a:

Grado de adopción y retención

Participación y simulación de oleadas

Detección de contactos estrechos

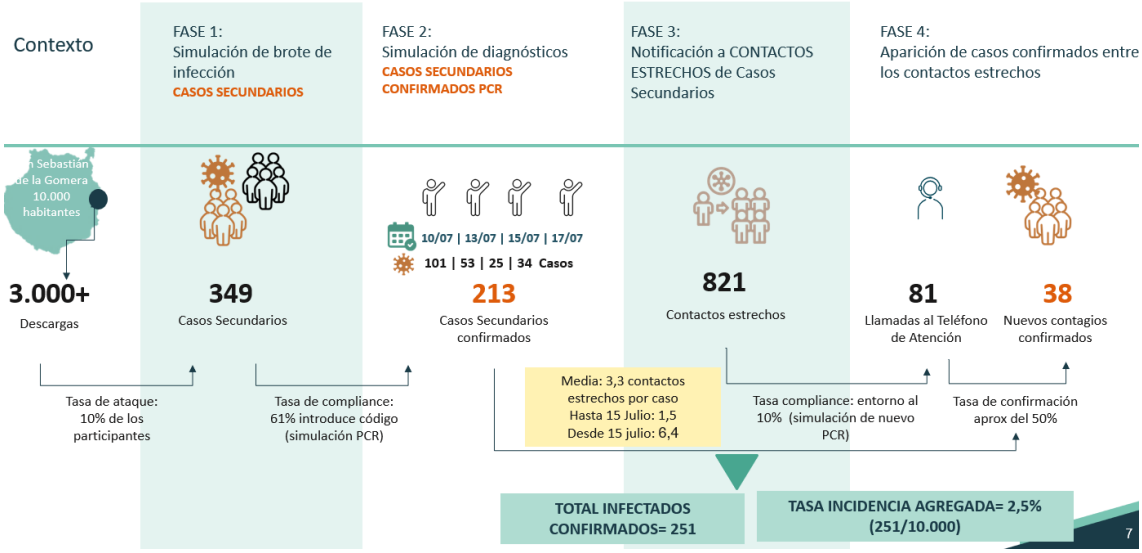
Feedback de usuarios

Resultados del piloto. ¿Qué conclusiones extraemos sobre el éxito del piloto?

Los usuarios continúan utilizando Radar COVID una vez instalada, como muestra el registro de apps activas: 12.700 Aplicaciones activas de media, con una variación de +/-5% entre sus máximos y mínimos (13.417 y 12.116)

Radar COVID es efectivo detectando contactos estrechos desde su recalibrado el día 15 de julio, al poder detectar contactos de personas cercanas al usuario y desconocidos*

Respecto a la "Simulación de brote Aplicación Radar COVID: datos finales" se informa:



¿Qué recomendaciones o enseñanzas de utilidad extraemos de cara a un escalado nacional?

Análisis:

- *Instrumentación para recopilación de datos anónimos para analizar el desempeño de Radar COVID con mayor precisión que la que la anonimidad total actual facilita.*
- *Calibrado: <u>seguimiento estadísticas agregadas</u> y de llamadas al call center para calibrado de pesos del Bluetooth de forma que se evite generar sobrealerta sin renunciar a un volumen útil de notificaciones de contacto estrecho generadas.*

<u>VIGÉSIMO:</u> Con fecha 27 de julio de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Constan como asistentes:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
A.A.A.	*SEDIA*
B.B.B.	*SEDIA*
C.C.C.	*SEDIA*

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
D.D.D.	*SEDIA*
E.E.E.	*Mº Sanidad*
F.F.F.	*Mº Sanidad*
G.G.G.	*SEDIA*
H.H.H.	*Gobierno de Canarias*
I.I.I.	*Minsait*
J.J.J.	*Minsait*
L.L.L.	*Minsait*
M.M.M.	*Minsait*
N.N.N.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*

Asuntos tratados:

Se presenta el documento anexo 20200721_Seguimiento SEDIA v5 dónde se recoge el resumen ejecutivo de las conclusiones del análisis de resultados del piloto.

Acuerdos adoptados:

Se acuerda tener listo para el próximo martes día 28/07/2020 el listado de acciones a llevar cabo sobre la app de cara a una puesta en producción inminente, ya sea en una CCAA, ciudad o a nivel nacional. Se acuerda también preparar un documento descriptivo con un resumen del funcionamiento de la app para que las diferentes CCAA puedan analizar su funcionamiento.

VIGÉSIMO PRIMERO: Consta un documento denominado "Radar COVID. Seguimiento de proyecto 31.07.2020", donde la SEDIA define las actividades de lanzamiento recomendadas para el roll out:

SEDIA / MINSAIT	COMUNIDADES AUTÓNOMAS	MINISTERIO DE SANIDAD
Personalización datos de contacto de CCAA –información usuario y atención positivos	Difusión de aplicación en CCAA para favorecer la adopción: Rueda de prensa, RRSS, promotores locales, medios de comunicación, webs oficiales…	Validación Informe de Análisis de Conclusiones
Eliminar encuesta usuario	Habilitar teléfono de atención y correo electrónico para consultas relacionadas con aplicación	Validación guía de app para Mº Sanidad
Eliminar referencias piloto la Gomera	Facilitar teléfono y dirección de correo electrónico a utilizar para la personalización de CCAA	Grupo de trabajo **Mº Sanidad** + CCAA + SEDIA (procedimientos, gestión códigos, protocolos actuación, …)
Certificado publicación app	Definir flujo de reporte y gestión de notificaciones de riesgo de alerta de contagio	Limitar a 5 días previos a la introducción de código el listado de claves positivas enviadas al servidor central
Subir "5" días de TEKs (verificar con MS)	Diseñar y gestionar circuito interno de códigos positivos (distribución, control y registro)	Enviar al servidor el listado de claves positivas desde 2 días anteriores al comienzo de síntomas
Cambiar nomenclatura de estados actuales	Revisar KPIs a implantar revisar	¿Incorporar grupo REDETS?
Multiidioma: Inglés	Definir interlocutor técnico por cada CCAA	
Traducción de textos de la aplicación a inglés	En caso de apoyo de agentes promotores, formación sobre aplicación y resolución de dudas	
Dosier remitido AEPD	Diseñar y coordinar comunicaciones directas con stakeholders clave de la CCAA	
Generar y enviar listado cifrado de códigos positivos a gestionar por la CCAA	Definir sistema de reporte y control de actividad derivada de APP.	
Revisión política de privacidad y términos de uso para eliminar referencias a piloto.	Establecer un mecanismo de obtención de feedback sobre funcionamiento e impacto de la APP en usuarios y sistema de salud	
Confirmar apertura con Google /Apple	Automatización de KPIs	
Documento app desde punto de vista Sanidad		

Actividades recomendadas

VIGÉSIMO SEGUNDO: Con fecha 3 de agosto de 2020 el METD publica esta nota de prensa:

"La aplicación móvil de alerta de contagios Radar COVID supera su fase de pruebas cumpliendo todos los objetivos marcados. (…)

Es lo que ha explicado la secretaria de Estado de Digitalización e Inteligencia Artificial, Carme Artigas, en una rueda de prensa en la que ha compartido los resultados obtenidos durante el piloto. Junto a ella han intervenido también Pilar Aparicio, directora general de Salud Pública e Innovación del Ministerio de Sanidad, S.S.S., director general de Modernización y Calidad de los Servicios del Gobierno de Canarias, D.D.D., subdirector general de Impulso de la Digitalización de la Administración, y C.C.C., asesor técnico del proyecto."

Éxito de adopción, compromiso, retención y funcionamiento.

La prueba arrancó el pasado 29 de junio y se ha desarrollado hasta este pasado 31 de julio, tiempo durante el que se han simulado cuatro oleadas de rebrotes ficticios de COVID-19. Durante su desarrollo, y a pesar de que sólo funcionaba en la isla de La Gomera, más de 60.000 personas descargaron la app en toda España.

El primer objetivo del piloto consistía en evaluar precisamente la adopción de la herramienta, es decir, el número de personas que la descargarían, y se fijó un objetivo de 3.000 participantes para La Gomera, meta que ha sido superada según los datos obtenidos durante la prueba.

Un segundo objetivo consistía en medir la retención, en referencia al número de usuarios que mantuvieron la app activa después de haberla descargado. Los resultados, también satisfactorios, apuntan a un 83% promedio de retención alcanzada.

Además, se analizaba el compromiso de los usuarios en la comunicación de positivos ficticios, lográndose un 61% de comunicaciones activas, de las que el 78% se produjeron en las 24 horas siguientes a haber recibido el código de contagio simulado.
Otro de los objetivos trazados en el piloto fue medir el funcionamiento de la app

en el traceo de contactos, consiguiendo una media de 6,4 contactos estrechos de riesgo detectados por positivo simulado confirmado. Esa cifra supone casi doblar la eficiencia actual de los traceadores manuales, que en Canarias detectan una media de 3,5 contactos. (…)

VIGÉSIMO TERCERO: Con fecha 5 de agosto de 2020 se celebra una reunión que tiene por objeto el "Diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por el Covid-19".

Constan como asistentes:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
A.A.A.	*SEDIA*
C.C.C.	*SEDIA*
D.D.D.	*SEDIA*
T.T.T.	*SEDIA*
F.F.F.	*Mº Sanidad*
V.V.V.	*CCAES*
W.W.W.	*CCAES*
I.I.I.	*Minsait*
J.J.J.	*Minsait*
L.L.L.	*Minsait*
M.M.M.	*Minsait*
X.X.X.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*

Acuerdos adoptados:

Se acuerda tener listo para el lunes día 10/08/2020 la app introduciendo los cambios comentados en el documentos anexo facilitando una salida de emergencia en el corto plazo a aquellas CCAA que lo soliciten y seguir avanzando en el desarrollo de las versiones para salida a nivel nacional.

VIGÉSIMO CUARTO: Con fecha 5 de agosto de 2020 se publica en el Boletín Oficial del Estado el Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, y se modifica el Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

En el preámbulo del real decreto 735/2020, se dice:

"(…) Para poder acometer de manera eficaz estas nuevas medidas, así como con el fin de hacer frente al incremento del volumen de trabajo en el Ministerio de Sanidad a raíz de la pandemia ocasionada por el COVID-19, se hace necesario reforzar la estructura de dicho Departamento. Por ello, mediante el Real De-

creto 722/2020, de 31 de julio, por el que se modifica el Real Decreto 2/2020, de 12 de enero, por el que se reestructuran los departamentos ministeriales, se dispuso la creación de una nueva Secretaría de Estado de Sanidad, con el objetivo de fortalecer el ejercicio de las competencias en materia de sanidad reservadas constitucionalmente a la Administración General del Estado.

Mediante el presente real decreto se refuerza adicionalmente la estructura del Ministerio de Sanidad, contemplándose la creación de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, de la que dependerá la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, con el objetivo de abordar los proyectos de modernización, mejora y transformación del Sistema Nacional de Salud, a la luz de los nuevos retos derivados de la pandemia ocasionada por el COVID-19, y en particular los relacionados con la salud digital, la interoperabilidad y los servicios en red en el ámbito nacional, europeo e internacional, así como los sistemas de información sanitarios, fomentando la incorporación de las prestaciones de las tecnologías emergentes de última generación, tales como el análisis de datos («big data»), la inteligencia artificial o la analítica predictiva, entre otros, en el ámbito de la salud."

Asimismo, la Disposición final primera del real decreto 735/2020 dispone:

"Modificación del Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales.

Se modifica el artículo 16 del Real Decreto 139/2020, de 28 de enero, por el que se establece la estructura orgánica básica de los departamentos ministeriales, que queda redactado como sigue:

«Artículo 16. Ministerio de Sanidad.

1. El Ministerio de Sanidad se estructura en los siguientes órganos superiores y directivos:

A) La Secretaría de Estado de Sanidad, de la que dependen los siguientes órganos directivos:

1.º La Dirección General de Salud Pública.

2.º La Dirección General de Cartera Común de Servicios del Sistema Nacional de Salud y Farmacia.

3.º La Dirección General de Ordenación Profesional.

4.º La Delegación del Gobierno para el Plan Nacional sobre Drogas, con rango de Dirección General.

B) La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, con rango de Subsecretaría, de la que depende la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud.

C) La Subsecretaría de Sanidad, de la que depende la Secretaría General Técni-

ca.

2. Quedan suprimidas la Secretaría General de Sanidad y Consumo y la Secretaría General de Sanidad, así como la Dirección General de Salud Pública, Calidad e Innovación y la Dirección General de Cartera Básica de Servicios del Sistema Nacional de Salud y Farmacia."

Las funciones de la DGSP constan en el artículo 3 del real decreto 735/2020 que dice:

1. La Dirección General de Salud Pública es el órgano que asume las funciones relativas a la sanidad exterior; la promoción de la salud y la prevención de las enfermedades y lesiones; la coordinación de la vigilancia en salud pública; (…).

Se constata que, la previsión que se contenía en el Real Decreto 454/2020, de 10 de marzo, en el artículo 3.2 relativa a que "Le corresponde la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica", ahora es atribuida a la SGSDII en el artículo 7.1 del real decreto 735/2020, que dice:

Artículo 7. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

1. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud es el órgano directivo del Departamento al que corresponde abordar los proyectos de modernización, innovación, mejora y transformación del Sistema Nacional de Salud a la luz de los nuevos retos derivados de la pandemia por COVID-19, en particular los relacionados con la salud digital y los sistemas de información. Asimismo, le corresponde la realización de actividades tendentes a la traslación de la innovación y avances de la investigación al Sistema Nacional de Salud, sin perjuicio de las competencias atribuidas al Ministerio de Ciencia e Innovación y a las comunidades autónomas. Le corresponde, igualmente, la elaboración de los sistemas de información, la gestión de la información y la identificación de la población protegida y el acceso a la información clínica y terapéutica. Igualmente le compete el control de la información sanitaria, en el ámbito de competencias del Departamento.

Se constatan las siguientes competencias a favor de la SGSDII atribuidas en los apartados d) y j) del artículo 7.4 del real decreto 735/2020:

d) Realizar las actuaciones necesarias para el desarrollo y mantenimiento del Sistema de Información Sanitaria del Sistema Nacional de Salud definido en el capítulo V de la Ley 16/2003, de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud, garantizando su normalización, comparabilidad, transparencia y accesibilidad dentro del marco legal de protección de datos personales. (…)

j) Coordinar y supervisar la política de protección de datos en cumplimiento de la normativa aplicable en esta materia en el ámbito de las competencias del Departamento.

Se constata que la SGSDII no interviene en el desarrollo del proyecto piloto dado

que se crea con el Real Decreto 735/2020, de 4 de agosto.

VIGÉSIMO QUINTO: En la versión inicial de la "Política de Privacidad de la Aplicación Radar COVID" publicada el día 7 de agosto de 2020 junto con la versión 1.0 de la aplicación Radar COVID (versión piloto), consta la siguiente información:

Por favor, lee detenidamente esta política de privacidad para usuarios de la aplicación móvil "Radar COVID" (o la "Aplicación"), donde podrás encontrar toda la información sobre los datos que utilizamos, cómo lo usamos y qué control tienes sobre los mismos.

AVISO IMPORTANTE:

El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. ¿Qué es Radar COVID?

Radar COVID es una aplicación para dispositivos móviles de alerta de contagios del virus SARS-CoV-2, cuyo TITULAR es la Secretaría General de Administración Digital, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Gracias a Radar COVID, aquellos usuarios que se hayan descargado la aplicación y acepten su uso recibirán una notificación en caso de que en los catorce días anteriores a esa notificación hayan estado expuestos a un contacto epidemiológico (a menos de dos metros y más de 15 minutos) con otro usuario (totalmente anónimo) que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias). La aplicación le informará exclusivamente sobre el día (dentro de esos catorce anteriores) en que se haya producido la exposición al contacto pero no sobre la identidad del usuario al que haya quedado expuesto (información imposible al ser una aplicación que no solicita, utiliza ni almacena datos de carácter personal de los usuarios) ni la identificación del dispositivo de este, ni sobre el momento o lugar en que la exposición se haya producido.

Recibida una notificación, la aplicación facilitará al usuario expuesto información para la adopción de medidas preventivas y asistenciales, para contribuir con ello a contener la propagación del virus.

El éxito de la aplicación como herramienta que contribuya a la contención de la propagación está directamente vinculado a que los usuarios sean conscientes, y actúen en consecuencia, de que, a pesar de que comunicar a la aplicación que se ha obtenido un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias) es voluntario, el no comunicarlo y ser un mero receptor de información de terceros usuarios hace que la aplicación pierda su utilidad preventiva no solo para los demás usuarios sino para el resto de la población en general. El carácter completamente anónimo debería animar, sin

duda, al ejercicio de esta actuación responsable.

2. ¿Cómo funciona la aplicación?

Una vez que te hayas descargado la aplicación, aceptes las condiciones de uso y la política de privacidad y comiences a utilizarla, tu dispositivo móvil generará cada día un identificador pseudo-aleatorio llamado "clave de exposición temporal" con un tamaño de 16 caracteres (16 bytes o 128 bits) que servirá para derivar los "identificadores efímeros Bluetooth" que son intercambiados con otros teléfonos móviles próximos que también tengan descargada la aplicación Radar-COVID.

Los "identificadores efímeros Bluetooth" son códigos pseudo-aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por tu teléfono móvil cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Estos códigos no contienen información personal, que permita identificar al teléfono móvil o al usuario del mismo. Estos "identificadores efímeros Bluetooth" son transmitidos por tu teléfono móvil varias veces por segundo a dispositivos cercanos, accesibles a través de Bluetooth Low Energy, produciendo un intercambio de códigos aleatorios entre dispositivos para que puedan ser almacenados por teléfonos próximos que hayan descargado la aplicación. De igual manera, cada cinco minutos, tu teléfono móvil escuchará los identificadores efímeros Bluetooth que son transmitidos por otros teléfonos móviles que tengan la aplicación y los almacenará para calcular si has estado con otro usuario contagiado por COVID-19 a lo largo de los últimos 14 días.

Tu teléfono almacena las claves de exposición temporal que has generado en los últimos 14 días. Recuerda que estas claves se generan aleatoriamente y no sirven para identificar a tu teléfono móvil ni al USUARIO del mismo.

Si has recibido un diagnóstico positivo por COVID-19, puedes introducir voluntariamente en la aplicación el "código de confirmación de un solo uso" que te facilitará tu Servicio Público de Salud y que será validado en nuestro servidor. En ese momento, la aplicación te solicitará tu consentimiento para remitir a nuestro servidor las 14 últimas claves de exposición temporal almacenadas en tu teléfono, por tanto, solo si lo prestas, éstas se enviarán al servidor de la aplicación que, después de verificar la exactitud del código, servirán para componer un listado diario de claves de exposición temporal de personas contagiadas por COVID-19 que son descargados diariamente desde el servidor por todas las aplicaciones Radar COVID que estén en funcionamiento.

La información de estos listados sirve para que en tu propio teléfono se pueda comprobar si has tenido contacto estrecho (menos de dos metros y más de 15 minutos) con personas que han reportado un contagio por COVID-19, sin identificar ni a la persona, ni el lugar de la exposición, ni el dispositivo móvil, ni ningún dato personal tuyo o de la otra persona. Es decir, la aplicación descarga periódicamente las claves de exposición temporal compartidas voluntariamente por los usuarios diagnosticados por COVID-19 del servidor, para compararlas con los códigos aleatorios registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo en el dispositivo que, en función de la duración y la distancia estimada del contacto, y de acuerdo con los criterios establecidos por las autoridades sanitarias, decide si se muestra una notificación en el dispositivo del usuario expuesto al riesgo de contagio, advirtiéndole del contacto, comunicándole la fecha

del mismo e invitándolo a auto-confinarse, y contactar con las autoridades sanitarias.

Estas claves remitidas al servidor no permiten la identificación directa de los usuarios y son necesarias para garantizar el correcto funcionamiento del sistema de alerta de contagios

3. ¿Qué datos tratamos sobre ti?

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para el único fin de informarte de que has estado expuesto a una situación de riesgo de contagio por la COVID-19, así como para facilitar la posible adopción de medidas preventivas y asistenciales.

En ningún caso se rastrearán los movimientos de los USUARIOS, excluyendo así cualquier forma de geolocalización.

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del USUARIO, y se suben al servidor para que puedan ser descargadas por aplicaciones similares en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al USUARIO sobre el riesgo de contagio por haber estado en contacto reciente con una persona que ha sido diagnosticada por COVID-19, sin que la aplicación pueda derivar su identidad o el lugar donde tuvo lugar el contacto.

Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por COVID-19. Este código debe ser informado por el usuario para permitir la carga voluntaria de las claves de exposición al servidor.

Cuestionario voluntario para la recogida de información sobre la experiencia de uso de la aplicación, comprensión de la misma o percepción sobre la privacidad entre otros.

Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad.

La legislación aplicable se enumera a continuación:

Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley 14/1986, de 25 de abril, General de Sanidad

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID-19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.

Orden Ministerial SND/297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

4. ¿Cómo obtenemos y de dónde proceden tus datos?

El código de confirmación de positivo por COVID-19 facilitado por el Servicio Público de Salud. Esto permitirá la subida al servidor del sistema de alerta de contagios las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves únicamente se suben al servidor con el consentimiento explícito e inequívoco del USUARIO, al haber introducido un código de confirmación de positivo por COVID-19.

5. ¿Para qué y por qué utilizamos tus datos?

La recogida, almacenamiento, modificación, estructuración y en su caso, eliminación, de los datos generados, constituirán operaciones de tratamiento llevadas a cabo por el Titular, con la finalidad de garantizar el correcto funcionamiento de la App, mantener la relación de prestación del servicio con el Usuario, y para la gestión, administración, información, prestación y mejora del servicio.

La información y datos recogidos a través de la Aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades:

Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después.

6. ¿Durante cuánto tiempo conservamos tus datos?

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

En todo caso, ni las claves de exposición temporal ni los identificadores efímeros de Bluetooth contienen datos de carácter personal ni permiten identificador los teléfonos móviles de los usuarios.

7. ¿Quién tiene acceso a tus datos?

Ni la aplicación "Radar COVID" ni el servidor de alerta de contagios almacenan datos personales de ningún tipo.

Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y derivar informes al USUARIO sobre su riesgo de exposición a la COVID-19.

Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.

Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.

8. ¿Cuáles son tus derechos y cómo puedes controlar tus datos?

Dado que la aplicación Radar COVID no almacena datos personales, no son de aplicación los derechos de acceso, rectificación, supresión, limitación, oposición y portabilidad, así como a no ser objeto de decisiones basadas únicamente en el tratamiento automatizado de sus datos.

En todo caso, tenemos obligación de indicarte que te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos (www.aepd.es).

9. ¿Cómo protegemos tus datos?

El sistema Radar COVID no almacena datos personales.

En todo caso, las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Finalmente, te informamos que tanto el almacenamiento como el resto de las ac-

tividades del tratamiento de datos no personales utilizados estarán siempre ubicados dentro de la Unión Europea.

10. ¿Cuál es la legitimación para el tratamiento de tus datos?

Los datos generados se tratarán legítimamente con las siguientes bases legales:

El consentimiento del usuario libre, específico, informado e inequívoco del USUARIO, poniendo a su disposición la presente política de privacidad, que deberá aceptar mediante el marcado de la casilla dispuesta al efecto.

Razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud (artículo 9.2 i) del RGPD), para el tratamiento de los datos de salud (por ejemplo, el estado de una persona contagiada o información sobre síntomas, etc.).

Cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento (artículo 6.1 e) RGPD).

Fines de archivo de interés público, fines de investigación científica o histórica o fines estadísticos (artículo 9.2 j) RGPD).

El Titular de la Aplicación podrá dar acceso o transmitir los datos a terceros proveedores de servicios, con los que haya suscrito acuerdos de encargo de tratamiento de datos, y que únicamente accedan a dicha información para prestar un servicio en favor y por cuenta del Responsable.

11. ¿Qué tienes que tener especialmente en cuenta al utilizar "Radar COVID"?

Has de tener en cuenta determinados aspectos relativos a la edad mínima de utilización de Aplicación, la calidad de los datos que nos proporcionas, así como la desinstalación de la Aplicación en tu dispositivo móvil.

Edad mínima de utilización: para poder utilizar “Radar COVID” tienes que ser mayor de 18 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en la Aplicación, garantizas al Titular que eres mayor de dicha edad o, en caso contrario, que cuentas con la mencionada autorización.

Calidad de los datos que nos proporcionas: la información que nos facilites en el uso de los servicios de la Aplicación deberá de ser siempre real, veraz y estar actualizada.

Desinstalación de la Aplicación: en general, puede haber dos situaciones en las que se proceda a la desactivación técnica de la Aplicación en tu dispositivo: 1) que lo realices voluntariamente, y 2) que desde el Titular se proceda a la desactivación técnica de la Aplicación en tu dispositivo (p.ej. en casos en los que detectemos que has incumplido las condiciones de uso de la Aplicación).

12. Política de cookies

Utilizamos solamente cookies técnicas que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen en la Aplicación como, por ejemplo, acceder a partes de acceso restringido o utilizar elementos de seguridad durante la navegación.

He leído el documento POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN “Radar COVID”.

VIGÉSIMO SEXTO: En la versión inicial de las "Condiciones de Uso de Radar COVID" consta la siguiente información:

CONDICIONES DE USO DE Radar COVID

AL DESCARGAR Y USAR LA APLICACIÓN MÓVIL "Radar COVID" MANIFIESTAS QUE HAS LEÍDO Y ACEPTAS ESTAS CONDICIONES DE USO Y LA POLÍTICA DE PRIVACIDAD. AQUÍ SE RECOGE TODA LA INFORMACIÓN RELATIVA A TUS DERECHOS Y OBLIGACIONES COMO USUARIO DE ESTA APLICACIÓN.

AVISO IMPORTANTE:

• El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. Qué es Radar COVID

Radar COVID es una aplicación que promueve la salud pública mediante un sistema de alerta de contagios por la COVID-19, poniendo a disposición de los USUARIOS (en adelante, individualmente, el "USUARIO", y conjuntamente los "USUARIOS"), la posibilidad de navegar por la Aplicación, accediendo a los contenidos y servicios de Radar COVID, de acuerdo con las presentes CONDICIONES DE USO.

Radar COVID detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación activa, mediante el empleo de identificadores aleatorios efímeros, que no guardan relación con la identidad del teléfono móvil empleado o el USUARIO. El dispositivo de cada USUARIO descarga periódicamente las claves Bluetooth de todos los USUARIOS de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias), procediendo a determinar si el USUARIO ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a evitar que el virus se propague.

2. Uso de Radar COVID

Para la utilización de los servicios de Radar COVID, es requisito necesario que el USUARIO autorice la activación del sistema de comunicaciones Bluetooth de baja energía por parte de la Aplicación, tras la descarga de la misma.

El USUARIO acepta sin reserva el contenido de las presentes CONDICIONES DE USO. En consecuencia, el USUARIO deberá leer detenidamente las mismas antes del acceso y de la utilización de cualquier servicio de Radar COVID bajo su entera responsabilidad.

AVISO IMPORTANTE: La utilización de la Aplicación es gratuita, libre y voluntaria para todos los ciudadanos. Para utilizar Radar COVID no es necesario estar registrado, ni aportar ningún dato personal, identificativo o no identificativo. Al activar la aplicación, el USUARIO acepta:

a) envío de señales Bluetooth emitidas de forma anónima por su dispositivo;

b) la recepción y almacenamiento de señales Bluetooth de aplicaciones compatibles con Radar COVID, que se mantienen de forma anónima y descentralizada en los dispositivos de los USUARIOS durante un periodo no superior a 14 días;

y c) la información ofrecida al USUARIO sobre el posible riesgo de contagio, sin que en ningún momento se refieran datos personales de ningún tipo.

El USUARIO puede informar voluntariamente a la aplicación de un resultado positivo en sus pruebas de COVID-19 mediante el código de confirmación de un solo uso facilitado por las autoridades sanitarias. La validez de este código será cotejada por las autoridades sanitarias para asegurar el correcto funcionamiento de Radar COVID. El USUARIO informará de los resultados de sus pruebas y se le solicitará el consentimiento expreso e inequívoco para compartir las claves generadas diariamente en su dispositivo, y correspondientes a los últimos 14 días. Estas claves son comunicadas a un servidor que las pondrá a disposición del conjunto de aplicaciones Radar COVID para su descarga. Las claves comunicadas no guardan relación alguna con la identificación del dispositivo o el USUARIO.

No se producirá ninguna discriminación a los potenciales pacientes que requieran servicios sanitarios y no hayan utilizado la aplicación.

3. Seguridad y privacidad

Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Te informamos que tus datos serán tratados conforme a lo establecido en la Política de Privacidad de la Aplicación, cuyo contenido íntegro se puede consultar en el siguiente enlace: Política de Privacidad.

Toda la información se tratará con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en la política de privacidad.

La información de la actividad de los USUARIOS es anónima y en ningún momento se exigirá a los USUARIOS ningún dato personal. En todo momento, el USUARIO puede desactivar el sistema de traza de contactos Bluetooth en la aplicación, así como desinstalar la misma.

4. Cambio del servicio y terminación

Radar COVID siempre está tratando de mejorar el servicio y busca ofrecer funcionalidades adicionales útiles para el USUARIO teniendo siempre presente la preservación de la salud pública. Esto significa que podemos añadir nuevas funciones o mejoras que en ningún caso implicarán el tratamiento de datos personales, así como eliminar algunas de las funciones. Si estas acciones afectan materialmente a los derechos y obligaciones del USUARIO, será informado a través de la Aplicación.

El USUARIO puede dejar de utilizar la aplicación en cualquier momento y por cualquier motivo, desinstalándola de su dispositivo.

5. Titular de la aplicación

La Secretaría General de Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, es la TITULAR de la aplicación Radar COVID.

Radar COVID en su arquitectura emplea el nuevo marco proporcionado por Apple y Google desarrollado a partir del Protocolo de DP-3T de rastreo de proximidad descentralizado para preservar la privacidad.

6. Responsabilidad y obligaciones

Radar COVID se ofrece dedicando los mejores esfuerzos, dado que su calidad y disponibilidad pueden verse afectadas por múltiples factores ajenos al TITULAR como son, entre otros, el volumen de USUARIOS en la ubicación geográfica del USUARIO, limitaciones o restricciones de las redes de terceros operadores o la compatibilidad del dispositivo y sistema operativo utilizado por el USUARIO. Igualmente, los USUARIOS aceptan que el servicio pueda verse interrumpido cuando sea necesario por labores de mantenimiento.

Por todo ello, el TITULAR no será responsable de los problemas de acceso o disponibilidad de Radar COVID y/o sus servicios, ni de los perjuicios que se pudieran causar por ello, cuando éstos procedan de factores ajenos a su ámbito de control. Igualmente, el TITULAR no se hace responsable de los siguientes hechos, ni de fallos, incompatibilidades y/o daños de tus terminales o dispositivos que, en su caso, se pudiesen derivar de la descarga y/o uso de la Aplicación:

- *Actualización, exactitud, exhaustividad, pertinencia, actualidad y fiabilidad de sus contenidos, cualquiera que sea la causa y las dificultades o problemas técnicos o de otra naturaleza en los que tengan su origen dichos hechos.*

- *La calidad, titularidad, legitimidad, adecuación o pertinencia de los materiales, y demás contenidos.*

Como USUARIO de la Aplicación te obligas a:

- *Impedir el acceso de terceras personas no autorizadas a la aplicación desde tu dispositivo.*

- *Notificar al TITULAR con carácter inmediato cualquier indicio de la existencia de una violación en la seguridad en la Aplicación, de usos inapropiados o prohibidos de los servicios prestados desde la misma, o de fallos de seguridad de cualquier índole.*

- *Hacer buen uso de los contenidos, información y servicios prestados desde o a través de la Aplicación, conforme a la ley, la buena fe y a las buenas costumbres generalmente aceptadas, comprometiéndose expresamente a:*

o *Abstenerse de realizar prácticas o usos de los servicios con fines ilícitos, fraudulentos, lesivos de derechos o intereses del TITULAR o de terceros, infractores de las normas contenidas en el presente documento.*

o *Abstenerse de realizar cualquier tipo de acción que pudiera inutilizar, sobrecargar o dañar sistemas, equipos o servicios de la Aplicación o accesibles directa o indirectamente a través de esta.*

o *Respetar los derechos de propiedad intelectual e industrial del TITULAR y de terceros sobre los contenidos, información y servicios prestados desde o a través de la Aplicación, absteniéndose con carácter general de copiar, distribuir, reproducir o comunicar en forma alguna los mismos a terceros, de no mediar autorización expresa y por escrito del TITULAR o de los titulares de dichos derechos.*

o *No proporcionar información falsa en la Aplicación, siendo el único responsable de la comunicación real y veraz.*

o *No suplantar la personalidad de un tercero.*

El USUARIO de la Aplicación es el único responsable del uso que decida realizar de los servicios de Radar COVID. El incumplimiento de las obligaciones como USUARIO podrá implicar la baja inmediata de la Aplicación y/o sus servicios; todo ello sin derecho a recibir compensación de ningún tipo, y sin perjuicio de las correspondientes acciones legales a que por parte del TITULAR hubiere lugar.

El TITULAR no será responsable en ningún caso de la utilización indebida de Radar COVID y de sus contenidos, siendo el USUARIO el único responsable por los daños y perjuicios que pudieran derivarse de un mal uso de estos o de la infracción de lo dispuesto en las presentes condiciones en que pueda incurrir. El USUARIO se compromete a mantener indemne al TITULAR frente a las reclamaciones o sanciones que pudiera recibir de terceros, ya sean particulares o entidades públicas o privadas, por razón de dichas infracciones, así como frente a los daños y perjuicios de todo tipo que pueda sufrir como consecuencia de las mismas.

En cualquier caso, el TITULAR se reserva, en cualquier momento y sin necesidad de previo aviso, el derecho de modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de esta Aplicación, siempre que lo estime oportuno, siempre que dicho cambio no afecte a los principios y derechos de protección de datos, así como el derecho interpretar las presentes

condiciones, en cuantas cuestiones pudiera plantear su aplicación.

Asimismo, queda prohibida la reproducción, distribución, transmisión, adaptación o modificación, por cualquier medio y en cualquier forma, de los contenidos de Radar COVID o sus cursos (textos, diseños, gráficos, informaciones, bases de datos, archivos de sonido y/o imagen, logos y demás elementos de estos sitios), salvo autorización previa de sus legítimos titulares.

La enumeración anterior tiene mero carácter enunciativo y no es, en ningún caso, exclusivo ni excluyente en ninguno de sus puntos. En todos los supuestos, El TITULAR EXCLUYE CUALQUIER RESPONSABILIDAD POR LOS DAÑOS Y PERJUICIOS DE CUALQUIER NATURALEZA DERIVADOS DIRECTA O INDIRECTAMENTE DE LOS MISMOS Y DE CUALESQUIERA OTROS NO ESPECIFICADOS DE ANÁLOGAS CARACTERISTICAS.

El TITUTAR NO OFRECE NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA, LEGAL O VOLUNTARIA.

EL TITULAR EXCLUYE EXPRESAMENTE TODAS LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO, A TÍTULO ENUNCIATIVO, PERO NO LIMITATIVO, CUALQUIER GARANTÍA IMPLÍCITA O SANEAMIENTO DE VICIOS OCULTOS, COMERCIABILIDAD, CALIDAD SATISFACTORIA, TÍTULO, IDONEIDAD DEL PRODUCTO PARA UN PROPÓSITO EN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. ESTA EXCLUSIÓN DE RESPONSABILIDAD SÓLO SE APLICARÁ EN LA MEDIDA PERMITIDA POR LA LEY IMPERATIVA APLICABLE.

7. Enlaces

Radar COVID puede incluir dentro de sus contenidos enlaces con sitios pertenecientes y/o gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

El TITULAR no asume ninguna responsabilidad derivada de la existencia de enlaces entre los contenidos de Radar COVID y contenidos situados fuera de los mismos o de cualquier otra mención de contenidos externos a este sitio, exceptuando aquellas responsabilidades establecidas en la normativa de protección de datos. Tales enlaces o menciones tienen una finalidad exclusivamente informativa y, en ningún caso, implican el apoyo, aprobación, comercialización o relación alguna entre el TITULAR y las personas o entidades autoras y/o gestoras de tales contenidos o titulares de los sitios donde se encuentren, ni garantía alguna del TITULAR por el correcto funcionamiento de los sitios o contenidos enlazados.

En este sentido el USUARIO se obliga a poner la máxima diligencia y prudencia en el caso de acceder o usar contenidos o servicios de los sitios a los que acceda en virtud de los mencionados enlaces.

8. Hiperenlaces

No se admite la reproducción de páginas de Radar COVID mediante hiperenlace

desde otra Aplicación móvil o página web, permitiéndose exclusivamente el acceso desde la Aplicación.

En ningún caso se podrá dar a entender que el TITULAR autoriza el hiperenlace o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la web desde la que se produce el hiperenlace.

No se podrán realizar manifestaciones o referencias falsas, incorrectas o inexactas sobre las páginas y servicios del TITULAR.

Se prohíbe explícitamente la creación de cualquier tipo de navegador, programa, "browser" o "border environment" sobre las páginas de Radar COVID.

No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios a la moral y las buenas costumbres aceptadas, ni contenidos o informaciones ilícitas, en la página web desde la que se establezca el hiperenlace.

La existencia de un hiperenlace entre una página web y el Radar COVID no implica la existencia de relaciones entre el TITULAR y el propietario de esa página, ni la aceptación y aprobación de sus contenidos y servicios.

9. Ley aplicable y fuero

Las presentes condiciones de uso se regirán e interpretarán en todos y cada uno de sus extremos por la Ley Española. En aquellos casos en los que la normativa vigente no prevea la obligación de someterse a un fuero o legislación determinado, el TITULAR y los USUARIOS, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los juzgados y tribunales de Madrid capital (España).

10. Información corporativa y contacto

Dirección: Calle de Manuel Cortina, 2, 28010 Madrid

El soporte al USUARIO en caso de incidencias y/o reclamaciones será principalmente online y atendido a la mayor brevedad: soporte.radarcovid@covid19.gob.es

VIGÉSIMO SÉPTIMO: El 12 de agosto de 2020 se elabora por la SEDIA, y según afirma la propia SEDIA, el primer documento de EIPD respecto del proyecto piloto Radar Covid, "cuando se tomó la decisión de que se adaptase el proyecto piloto para su despliegue a nivel nacional".

En dicho documento se afirma la existencia de tratamientos de datos de carácter personal:

"Por tanto, en los casos en que, a primera vista, la información no permite singularizar a una persona determinada, esta aún puede ser identificable, porque esa información puede ser combinada con otros datos, tanto si el responsable de su tratamiento tiene conocimiento de ellos como si no, que permitan distinguir a esa persona de otras.

A pesar de que tradicionalmente los datos pseudonimizados eran considerados datos anónimos, en la actualidad la pseudonimización ya no se considera un método de anonimización, pues la persona es todavía identificable, aunque sea de forma indirecta. Así, actualmente se considera que los datos pseudonimizados son todavía datos de carácter personal y están sujetos a la normativa sobre protección de datos de carácter personal.

En conclusión, en este tratamiento, a pesar de que los usuarios no puedan ser identificados directamente, podrían llegar a ser identificables, realizándose mapas de relaciones entre personas, mediante reidentificación por localización implícita llegando, incluso, a poder identificar la identidad de los contagiados. Debe tenerse en cuenta, en este sentido, que el tratamiento de la información no solo afecta al usuario de la aplicación sino también a la de todos los terceros con los que ha estado en contacto.

Una vez dicho lo anterior, partiendo por tanto de que a la actividad de tratamiento en cuestión le aplica la normativa vigente sobre privacidad y protección de datos, y teniendo en cuenta la categoría de datos que podrían llegar a identificar a los usuarios, se procede a analizar la necesidad de realizar una EIPD".

En cuanto a los roles de "Responsables, corresponsables y encargados del tratamiento" dispone:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias, que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

En este caso el titular de la aplicación es la Secretaría General de Administración Digital dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que también se constituye como Responsable del Tratamiento.

La aplicación ha sido desarrollada a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA)".

Respecto de los datos personales tratados confirma los siguientes:

"De esta forma, los datos generados o a los que accede la aplicación, son los siguientes:

· La aplicación genera datos de proximidad (claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios o Identificador de proximidad rodante - RPI), que son datos generados mediante el intercambio de señales de Bluetooth de baja energía (BLE) entre dispositivos dentro de una distancia relevante desde el punto de vista epidemiológico y durante un tiempo relevante también desde el punto de vista epidemiológico. Estos datos se comunicarán a las autoridades sanitarias únicamente cuando se haya confirmado que un usuario en cuestión está infectado de COVID-19 y a condición de que la persona opte por que así se haga, es decir, de manera voluntaria.

· Dato mediante el que el usuario es advertido previamente de un contacto de riesgo. Estos datos permiten estimar cuántos usuarios son advertidos por la apli-

cación de un riesgo potencial de contagio, sin poder rastrear su identidad, y le permite al Servicio Nacional de Salud preparar las iniciativas y los recursos necesarios para atender a los usuarios que han recibido la notificación.

· El día en que el usuario desarrolló síntomas compatibles con COVID-19.

· Código (QR) proporcionado por las autoridades sanitarias para permitir al usuario activar una alerta de advertencia. Este número de 12 cifras será proporcionado por las autoridades sanitarias, que lo enviarán después de dar positivo. Este número no deja de ser la "confirmación" que efectivamente el usuario ha dado positivo y no se trata de un usuario aleatorio intentando enviar alertas falsas.

· La dirección IP que utiliza el dispositivo para conectarse a Internet. En este sentido cabe traer a colación la Sentencia del Tribunal Supremo de 3 de octubre de 2014, en cuyo Fundamento de Derecho número cuatro establece que «no cabe duda que, a partir de la dirección IP puede identificarse directa o indirectamente la identidad del interesado, ya que los proveedores de acceso a internet tienen constancia de los nombres, teléfono y otros datos identificativos de los usuarios a los que han asignado las particulares direcciones IP». La Sentencia confirma que las direcciones IP son datos personales ya que contienen información concerniente a personas identificadas o identificables.

(…)

Por tanto, como consecuencia de lo anterior, cualquier sistema de seguimiento de proximidad que verifique una base de datos pública de claves de diagnóstico contra identificadores cambiantes de proximidad (rolling proximity identifiers-RPID) en el dispositivo de un usuario deja abierta la posibilidad de que los contactos de una persona infectada descubran cuál de las personas que encontraron es infectado. Además, el hecho de que los usuarios infectados compartan públicamente sus claves de diagnóstico una vez al día, en lugar de sus RPID cada pocos minutos, expone a esas personas a ataques de enlace.

Por ello, hay que prestar especial atención a esta probabilidad ya que en el caso de que un usuario de la aplicación pudiera ser identificado, la privacidad quedaría enormemente amenazada, pudiendo resultar afectados todo tipo de datos personales como:

· Datos de salud,

· Localización,

· Contactos,

· Correo electrónico,

· Registro de llamadas,

· SMS y mensajería instantánea,

· Identidad del interesado,

· Identidad del teléfono (es decir, nombre del teléfono)

· Historial de navegación,

· Credenciales de autenticación para los servicios de la sociedad de la información (en particular los servicios con características sociales)

· Fotografías y vídeos

· Datos biométricos (por ejemplo, modelos de reconocimiento facial y huellas dactilares)".

Respecto de la finalidad del tratamiento, lo determinan, ligándolo a las funcionalidades de la aplicación:

"Cada una de las distintas funcionalidades de la aplicación obedece a determinados fines:

· La finalidad principal de la App es informar a las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus, a fin de romper las cadenas de transmisión lo antes posible. De esta manera, la aplicación permite identificar a las personas que han estado en contacto con alguien infectado por la COVID-19 e informarles de las medidas que conviene adoptar después, como someterse a autocuarentena o a las pruebas correspondientes.

· Para ello la App mantiene los contactos de las personas que utilizan la aplicación y que pueden haber estado expuestas a la infección de la COVID-19.

· Cuando una persona da positivo en el test de COVID-19 y decida compartir libremente este dato, la App alerta a aquellas otras personas que podrían haber sido infectadas y con las que se haya tenido contacto los últimos 14 días. Para ello, esta persona deberá compartir un número de 12 cifras que será proporcionado por las autoridades sanitarias. El móvil realiza una comprobación de si los ID aleatorios coinciden con alguno que haya sido marcado como positivo.

· Se determina el día en que el usuario desarrolló síntomas compatibles con COVID-19 y fecha de contacto con personas infectadas".

Del estudio del ciclo de vida de los datos se indica que la captura de los datos se produce con el "Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App".

VIGÉSIMO OCTAVO: Con fecha 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud, firma un "Acuerdo de uso de la aplicación "Radar COVID", en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas" que dice:

Para contribuir a estas tareas de búsqueda activa de contactos estrechos de casos confirmados, desde la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), se ha desarrollado, en coordinación con otros miembros de la UE y la red de eHealth, una herramienta digital para complementar las tareas de búsqueda manual de contactos que llevan a cabo los correspondientes servicios de las comunidades y ciudades autónomas. (…)
Durante el mes de julio de 2020, la Secretaría General de Administración Digital, órgano directivo dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial, llevó a cabo con éxito un proyecto piloto para comprobar el funcionamiento de esta aplicación en la isla de la Gomera. (…)
El presente Acuerdo temporal permite establecer los términos de uso por parte de las comunidades y ciudades autónomas de la aplicación "RADAR COVID" durante dicha fase de pruebas, hasta la fecha de total operatividad de la misma, que se producirá mediante la adhesión a la aplicación a través de los oportunos convenios bilaterales de la Secretaría de Estado de Digitalización e Inteligencia

Artificial con las diferentes comunidades y ciudades autónomas.

En el punto 5 se dice:

5. En relación con el tratamiento de datos de carácter personal, y en aplicación del régimen previsto en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE, durante la vigencia de este Acuerdo, el responsable del tratamiento será el Ministerio de Sanidad y, en su respectivo territorio, cada una de las comunidades y ciudades autónomas que se vayan incorporando durante la fase de pruebas al uso de la aplicación, ostentando plenamente sus competencias en materia sanitaria. El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial.

VIGÉSIMO NOVENO: Consta el Documento técnico "Procedimiento de implementación de la App Radar COVID como complemento a los sistemas manuales de identificación de contactos" en su versión de 14 de agosto de 2020, coordinado por:

- *Centro de Coordinación de Alertas y Emergencias Sanitarias.*
- *Dirección General de Salud Pública, Calidad e Innovación.*

TRIGÉSIMO: A nivel nacional, la puesta en servicio de la App Radar COVID se produce en fecha 19 de agosto de 2020.

TRIGÉSIMO PRIMERO: Con fecha 26 de agosto de 2020 se celebra la reunión para determinar la situación del proyecto y los próximos pasos. Los asistentes son:

Persona	*SEDIA / CCAA / Mº Sanidad / Minsait*
A.A.A.	*SEDIA*
C.C.C.	*SEDIA*
Y.Y.Y.	*SEDIA*
Dª T.T.T.	*SEDIA*
I.I.I.	*Minsait*
N.N.N.	*Minsait*
Ñ.Ñ.Ñ.	*Minsait*

TRIGÉSIMO SEGUNDO: Consta una primera versión del documento "Análisis de Riesgos Servicio Radar Covid19" fechado en agosto de 2020, elaborado por MINTSAIT an INDRA COMPANY.

TRIGÉSIMO TERCERO: Consta una segunda versión del documento "Análisis de Riesgos Servicio Radar Covid19" fechado en septiembre de 2020, elaborado por MINTSAIT an INDRA COMPANY.

El principal objetivo del Análisis de Riesgos es determinar el nivel de riesgo al que están expuestos los activos del Servicio Radar Covid19, teniendo en cuenta las amenazas a las que están expuestos y el nivel de eficacia de los controles implantados actualmente para protegerlos. El Análisis de Riesgos está basado en la información aportada por los responsables técnicos de INDRA y los responsables del desarrollo, puesta en marcha e implantación de la Aplicación Radar Covid19, quienes conocen la infraestructura y que, por tanto, pueden conocer el grado de implantación de cada una de las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad. Por otra parte, el presente documento se ha elaborado con la información recabada hasta su fecha de edición, por lo que, salvo indicación expresa, los cambios realizados después de esta fecha no se verán reflejados en el mismo. Como se ha comentado anteriormente, el nivel del riesgo se puede clasificar en una escala de 0 a 10, siendo el valor 0 el riesgo despreciable y el valor 10 el riesgo extremadamente crítico. Teniendo en cuenta dicha escala, y tomando como métrica para el nivel de riesgo el mayor valor de riesgo identificado en un activo, el resultado del Análisis de Riesgos determina un Nivel de Riesgo Actual = {2,6}. Atendiendo a los niveles mínimos de madurez requeridos por el Esquema Nacional de Seguridad y tomando para el riesgo objetivo la misma métrica que se ha tomado para el riesgo residual, es decir, el mayor valor de riesgo identificado en un activo, el objetivo que se propone alcanzar en el proceso de mitigación de riesgos quedaría establecido en un Nivel de Riesgo Objetivo = {1,8}.

Se recomienda abordar un conjunto de acciones para mejorar las medidas de seguridad existentes actualmente, con el objeto de ajustar el nivel de riesgo del Servicio Radar Covid19 a un nivel BAJO. Estas acciones se han focalizado en las medidas de seguridad que pueden minimizar las amenazas que aportan un nivel de riesgo MEDIO en el presente Análisis de Riesgos. Estas acciones permitirán alcanzar el nivel de Riesgo Objetivo propuesto, ya que aumentarían el grado de madurez de las medidas de seguridad Mp.info.4 Firma electrónica y Op.acc.5 Mecanismos de autenticación.

Las acciones propuestas en este caso son:

- Utilizar certificados cualificados para la firma digital que se utiliza en el servicio de verificación de los positivos.

- Verificar que los elementos criptográficos hardware del AWS Multi-Factor Authentication (MFA) utilizan algoritmos y parámetros acreditados por el CCN. Además se recomienda revisar el mecanismo de control de acceso a la Base de Datos PostgreSQL para concluir que cumple con los requisitos de nivel alto.

TRIGÉSIMO CUARTO Con fecha 9 de septiembre de 2020 el METD publica esta nota de prensa:

"La aplicación móvil RadarCOVID completa su implantación en trece comunidades autónomas, que abarcan el 70% de la población, y libera su código. (…)

A falta de esa necesaria integración, la aplicación está activa y funcionando en todo el territorio nacional desde el pasado mes de agosto. Eso implica que el terminal ya almacena los identificadores anónimos de los otros terminales con los

que se ha estado en contacto de riesgo durante los últimos siete días.

Por eso, y aunque la implementación técnica esté en proceso en algunas comunidades autónomas, es útil tener ya instalada la aplicación para que ese proceso de registro vaya teniendo lugar y poder estar así protegidos desde el primer momento en el que se pone en marcha. Más de 3,7 millones de usuarios han descargado ya la aplicación, protegiéndose y protegiendo a sus personas cercanas contra posibles cadenas de contagio.

Liberación del código

Además, se ha dado cumplimiento a uno de los compromisos adquiridos con el inicio del desarrollo de la aplicación: la liberación de su código.

Se trata de un ejercicio de transparencia para que el funcionamiento de la aplicación pueda ser auditado de forma abierta y directa por parte de la ciudadanía. (…)

Con la intención de dar a conocer el funcionamiento de la aplicación y resolver las dudas y cuestiones que la ciudadanía comparte a través de las redes sociales, la Secretaría de Estado de Digitalización e IA ha puesto en marcha dos cuentas específicas para la aplicación. Así, desde la cuenta @AppRadarCOVID, disponible tanto en Twitter como en Instagram, se irá compartiendo información puntual sobre las novedades respecto a la app y se dará respuesta a las preguntas más frecuentes que haga llegar la ciudadanía."

TRIGÉSIMO QUINTO: Consta el Documento técnico "Procedimiento de implementación de la App Radar COVID como complemento a los sistemas manuales de identificación de contactos" en su versión de 15 de septiembre de 2020, coordinado por:

- *Centro de Coordinación de Alertas y Emergencias Sanitarias.*
- *Dirección General de Salud Pública, Calidad e Innovación.*

TRIGÉSIMO SEXTO: Constan dos versiones más de la Evaluación de impacto:

En la segunda versión, fechada en septiembre de 2020, se dice:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias, que garantizarán la aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a COVID Radar 10 categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

En este caso el titular de la aplicación es la Secretaría General de Administración Digital dependiente del Ministerio de Asuntos Económicos y Transformación

Digital, que también se constituye como Responsable del Tratamiento".

En la tercera versión, se dice:

"Por ello, y en virtud de lo dispuesto en el artículo 27.3, los responsables del tratamiento serán las comunidades autónomas, las ciudades de Ceuta y Melilla y el Ministerio de Sanidad, en el ámbito de sus respectivas competencias, que garantizarán la Aplicación de las medidas de seguridad preceptivas que resulten del correspondiente análisis de riesgos, teniendo en cuenta que los tratamientos afectan a Radar COVID 10 categorías especiales de datos y que dichos tratamientos serán realizados por administraciones públicas obligadas al cumplimiento del Esquema Nacional de Seguridad.

El responsable de tratamiento es la Dirección General de Salud Pública, dependiente del Ministerio de Sanidad.

El encargado de tratamiento es la Secretaría General de Administración Digital, dependiente del Ministerio de Asuntos Económicos y Transformación Digital, que ha desarrollado la Aplicación."

Asimismo, en la primera versión de la Evaluación de impacto se indica respecto de su finalidad que "El presente documento tiene como objetivo exponer los resultados del Análisis de Riesgos realizado al Servicio Radar Covid19 respecto al Esquema Nacional de Seguridad".

Aseveran que "La aplicación no solicita ningún dato de carácter personal, ni requiere crear usuario (sin login ni datos personales). La aplicación utiliza claves anónimas e intercambia identificadores aleatorios, que están en constante cambio. El personal implicado en la aplicación conoce la tipología de la información y, lo más importante, la Política de Seguridad".

Conforme a lo anterior y al contenido de esta, la evaluación de impacto se limita a examinar el cumplimiento del ENS, sin entrar en un posible análisis de riesgos o evaluación de impacto de protección de datos.

TRIGÉSIMO SÉPTIMO: En la versión definitiva de la "Política de Privacidad de la Aplicación Radar COVID" publicada en octubre de 2020, consta la siguiente información:

POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN Radar COVID

Por favor, lee detenidamente esta política de privacidad para usuarios de la aplicación móvil "Radar COVID" (o la "Aplicación"), donde podrás encontrar toda la información sobre los datos que utilizamos, cómo lo usamos y qué control tienes sobre los mismos.

AVISO IMPORTANTE:

El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico de-

bidamente cualificado.

1. ¿Qué es Radar COVID?

Radar COVID es una aplicación para dispositivos móviles de alerta de contagios del virus SARS-CoV-2, cuyo TITULAR es la Secretaría General de Administración Digital, dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital.

Gracias a Radar COVID, aquellos usuarios que se hayan descargado la aplicación y acepten su uso recibirán una notificación en caso de que en los catorce días anteriores a esa notificación hayan estado expuestos a un contacto epidemiológico (a menos de dos metros y más de 15 minutos) con otro usuario (totalmente anónimo) que haya declarado en la aplicación haber dado un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias). La aplicación le informará exclusivamente sobre el día (dentro de esos catorce anteriores) en que se haya producido la exposición al contacto pero no sobre la identidad del usuario al que haya quedado expuesto (información imposible al ser una aplicación que no solicita, utiliza ni almacena datos de carácter personal de los usuarios) ni la identificación del dispositivo de este, ni sobre el momento o lugar en que la exposición se haya producido.

Recibida una notificación, la aplicación facilitará al usuario expuesto información para la adopción de medidas preventivas y asistenciales, para contribuir con ello a contener la propagación del virus.

El éxito de la aplicación como herramienta que contribuya a la contención de la propagación está directamente vinculado a que los usuarios sean conscientes, y actúen en consecuencia, de que, a pesar de que comunicar a la aplicación que se ha obtenido un resultado positivo en la prueba de COVID 19 (previa acreditación de las autoridades sanitarias) es voluntario, el no comunicarlo y ser un mero receptor de información de terceros usuarios hace que la aplicación pierda su utilidad preventiva no solo para los demás usuarios sino para el resto de la población en general. El carácter completamente anónimo debería animar, sin duda, al ejercicio de esta actuación responsable.

2. ¿Cómo funciona la aplicación?

Una vez que te hayas descargado la aplicación, aceptes las condiciones de uso y la política de privacidad y comiences a utilizarla, tu dispositivo móvil generará cada día un identificador aleatorio llamado "clave de exposición temporal" con un tamaño de 16 caracteres (16 bytes o 128 bits) que servirá para derivar los "identificadores efímeros Bluetooth" que son intercambiados con otros teléfonos móviles próximos que también tengan descargada la aplicación Radar COVID y activado su Bluetooth.

Los "identificadores efímeros Bluetooth" son códigos aleatorios con un tamaño de 16 caracteres (16 bytes, o 128 bits), que se generan por tu teléfono móvil cada 10-20 minutos, a partir de la "clave de exposición temporal" diaria. Estos códigos no contienen información personal, que permita identificar al teléfono móvil o al usuario del mismo. Estos "identificadores efímeros Bluetooth" son transmitidos por tu teléfono móvil varias veces por segundo a dispositivos cercanos, accesibles a través de Bluetooth de baja energía (BLE, Bluetooth Low Energy), produciendo un intercambio de códigos aleatorios entre dispositivos para que puedan ser almacenados por teléfonos próximos que hayan descargado la

aplicación. De igual manera, cada cinco minutos, tu teléfono móvil escuchará los identificadores efímeros Bluetooth que son transmitidos por otros teléfonos móviles que tengan la aplicación y los almacenará para determinar si has estado con otro usuario contagiado por COVID-19 a lo largo de los últimos 14 días que haya comunicado un positivo.

Tu teléfono almacena las claves de exposición temporal que has generado en los últimos 14 días. Recuerda que estas claves se generan aleatoriamente y no sirven para identificar a tu teléfono móvil ni al USUARIO del mismo.

Si has recibido un diagnóstico positivo por COVID-19, puedes introducir voluntariamente en la aplicación el "código de confirmación de un solo uso" que te facilitará tu Servicio Público de Salud y que será validado en el servidor de la SGAD. En ese momento, la aplicación te solicitará tu consentimiento para remitir a nuestro servidor hasta un máximo de las 14 últimas claves de exposición temporal almacenadas en tu teléfono, por tanto, solo si lo prestas, éstas se enviarán al servidor de la SGAD que, después de verificar la exactitud del código, servirán para componer un listado diario de claves de exposición temporal de personas contagiadas por COVID-19 que son descargados diariamente desde el servidor por todas las aplicaciones Radar COVID que estén en funcionamiento.

La información de estos listados sirve para que en tu propio teléfono se pueda comprobar si has tenido contacto estrecho (menos de dos metros y más de 15 minutos) con personas que han reportado un contagio por COVID-19, sin identificar ni a la persona, ni el lugar de la exposición, ni el dispositivo móvil, ni ningún dato personal tuyo o de la otra persona. Es decir, la aplicación descarga periódicamente las claves de exposición temporal compartidas voluntariamente por los usuarios diagnosticados por COVID-19 del servidor, para compararlas con los códigos aleatorios registrados en los días anteriores como resultado de contactos con otros usuarios. Si se encuentra una coincidencia, la aplicación ejecuta un algoritmo en el dispositivo que, en función de la duración y la distancia estimada del contacto, y de acuerdo con los criterios establecidos por las autoridades sanitarias, evalúa el riesgo de exposición al virus SARS-CoV-2 y en su caso muestra una notificación advirtiendo del contacto de riesgo al usuario, comunicándole la fecha del mismo e invitándolo a auto-confinarse y contactar con las autoridades sanitarias.

Estas claves remitidas al servidor no permiten la identificación directa de los usuarios y son necesarias para garantizar el correcto funcionamiento del sistema de alerta de contactos de riesgo.

3. ¿Quiénes son los responsables del tratamiento de tus datos como usuario de "Radar COVID"?

Esta aplicación tiene como responsables de tratamiento tanto al Ministerio de Sanidad, como a las Comunidades Autónomas. Así mismo, la Secretaría General de Administración Digital ejerce como encargada del tratamiento.

A nivel nacional, el responsable del tratamiento de tus datos como usuario de "Radar COVID" es:

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Nombre: Ministerio de Sanidad.

Dirección: Paseo del Prado 18-20, 28014 Madrid

La Secretaría General de Administración Digital, en calidad de titular de la aplicación y en base al encargo del tratamiento encomendado por el Ministerio de Sanidad, efectuará las siguientes operaciones del tratamiento:

Generación de códigos para la comunicación de positivos en la aplicación Radar COVID.

Recepción de la información remitida por los usuarios cuando comunican un positivo. Esta información incluye:

Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.

La preferencia o no por comunicar estas claves de exposición diaria al nodo europeo de interoperabilidad entre aplicaciones de rastreo de contactos.

Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID.

En relación al nodo europeo de interoperabilidad de contactos (EFGS).

Recepción diaria de los listados de claves de exposición temporal generados por los servidores nacionales de los Estados Miembros adheridos en su caso al proyecto.

Remisión diaria al nodo EFGS de un listado de claves de exposición temporal remitidas por los usuarios de Radar COVID que han consentido explícitamente compartir esta información con el resto de Estados Miembros adheridos al proyecto.

Las Comunidades Autónomas adheridas al uso de la aplicación son, así mismo, responsables del tratamiento, llevando a cabo las siguientes operaciones de tratamiento:

Solicitud al servidor Radar COVID de generación de códigos de confirmación de positivo.

Entrega de estos códigos a las personas diagnosticadas positivas por pruebas PCR.

El encargado del tratamiento y titular de la aplicación es la Secretaría General de Administración Digital, órgano directivo de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, en virtud al Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "Radar COVID".

4. ¿Qué datos tratamos sobre ti?

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para el único fin de informarte de que has estado expuesto a una situación de riesgo de contagio por la COVID-19, así como para facilitar la posible adopción de medidas preventivas y

asistenciales.

En ningún caso se rastrearán los movimientos de los USUARIOS, excluyendo así cualquier forma de geolocalización.

No se almacenará ni tratará la dirección IP de los USUARIOS.

No se almacenarán los códigos de confirmación de positivo junto con otros datos personales de los usuarios.

Como parte del sistema de alerta de contactos de riesgo de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID-19 para los fines especificados a continuación:

Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves no guardan relación alguna con la identidad del USUARIO, y se suben al servidor para que puedan ser descargadas por aplicaciones Radar COVID en poder de otros usuarios. Con estas claves, mediante un procesamiento que tiene lugar en el teléfono móvil de forma descentralizada, se puede advertir al USUARIO sobre el riesgo de contagio por haber estado en contacto reciente con una persona que ha sido diagnosticada por COVID-19, sin que la aplicación pueda derivar su identidad o el lugar donde tuvo lugar el contacto.

Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias al USUARIO en caso de prueba positiva por COVID-19. Este código debe ser introducido a continuación por el usuario en la aplicación para permitir la carga voluntaria al servidor de las claves de exposición temporal.

El consentimiento del usuario, si aplica, para la remisión de claves de exposición temporal al nodo europeo de interoperabilidad de aplicaciones de rastreo de contactos.

El aviso de notificación de exposición, a efectos de recoger una estadística anónima y agregada del volumen de notificaciones que produce el sistema a través del rastreo de contactos. Estos datos permiten estimar cuántos usuarios han sido alertados por la Aplicación, de un riesgo potencial de infección, sin poder rastrear su identidad.

Toda la información se recogerá con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en esta política de privacidad, y atendiendo a los artículos 6.1.a), 9.2.a), 6.1.c), 6.1.d), 6.1.e), 9.2.c), 9.2.h) y 9.2.i)

La legislación aplicable se enumera a continuación:

Reglamento (UE) 2016/679, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento General de Protección de Datos).

Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

Ley 33/2011, de 4 de octubre, General de Salud Pública.

Ley 14/1986, de 25 de abril, General de Sanidad.

Real Decreto ley 21/2020, de 9 de junio, de medidas urgentes de prevención, contención y coordinación para hacer frente a la crisis sanitaria ocasionada por el COVID-19.

Acuerdo de 9 de octubre de 2020, entre el Ministerio de Asuntos Económicos y Transformación Digital (Secretaría de Estado de Digitalización e Inteligencia Artificial) y el Ministerio de Sanidad acerca de la aplicación "Radar COVID".

5. ¿Cómo obtenemos y de dónde proceden tus datos?

El código de confirmación de positivo por COVID-19 facilitado por el Servicio Público de Salud. Esto permitirá la subida al servidor de las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth) a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores. Estas claves únicamente se suben al servidor con el consentimiento explícito e inequívoco del USUARIO, al haber introducido un código de confirmación de positivo por COVID-19.

El aviso de notificación de exposición es facilitado por la aplicación de forma anónima a los efectos de componer una estadística agregada del volumen de usuarios que han sido notificados.

6. ¿Para qué y por qué utilizamos tus datos?

La recogida, almacenamiento, modificación, estructuración y en su caso, eliminación, de los datos generados, constituirán operaciones de tratamiento llevadas a cabo por el Titular, con la finalidad de garantizar el correcto funcionamiento de la App, mantener la relación de prestación del servicio con el Usuario, y para la gestión, administración, información, prestación y mejora del servicio.

La información y datos recogidos a través de la Aplicación serán tratados con fines estrictamente de interés público en el ámbito de la salud pública, ante la actual situación de emergencia sanitaria como consecuencia de la pandemia del COVID-19 y la necesidad de su control y propagación, así como para garantizar intereses vitales tuyos o de terceros, de conformidad con la normativa de protección de datos vigente.

A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades:

Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuaren-

tena.

Se utilizarán los datos siempre y sólo de forma anonimizada para fines estadísticos y epidemiológicos.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después.

7. ¿Durante cuánto tiempo conservamos tus datos?

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

En todo caso, ni las claves de exposición temporal ni los identificadores efímeros de Bluetooth contienen datos de carácter personal ni permiten identificador los teléfonos móviles de los usuarios.

El aviso de notificación de exposición se agrega en el indicador de avisos diarios comunicados, siendo descartado para cualquier otro uso.

8. ¿Quién tiene acceso a tus datos?

Los datos gestionados por la aplicación móvil (claves diarias de exposición temporal e identificadores efímeros Bluetooth) se almacenan únicamente en el dispositivo del usuario a los efectos de poder hacer cálculos y avisar al USUARIO sobre su riesgo de exposición a la COVID-19.

Solo en el caso de reportar un diagnóstico positivo por COVID-19, las claves de exposición temporal de los últimos 14 días generadas en el dispositivo, y bajo el consentimiento explícito e inequívoco del USUARIO, son subidas al servidor para su difusión al conjunto de USUARIOS de este sistema.

Estas claves no guardan relación alguna con la identidad de los dispositivos móviles ni con datos personales de los USUARIOS de la Aplicación.

Los avisos de notificación de exposición comunicados solo se utilizan para la generación de datos estadísticos agregados y anónimos.

9. ¿Cuáles son tus derechos y cómo puedes controlar tus datos?

La normativa vigente te otorga una serie de derechos en relación con los datos e información que tratamos sobre ti. Concretamente, los derechos de acceso, rectificación, supresión, limitación y oposición.

Puedes consultar el alcance y detalle completo de los mismos en la página web de la Agencia Española de Protección de Datos (AEPD) aquí.

Con carácter general, podrás ejercitar todos estos derechos en cualquier momento y de forma gratuita. Puedes dirigirte a los Responsables de Tratamiento por vía electrónica, bien Ministerio de Sanidad o Comunidad Autónoma de residencia. En el caso del Ministerio de Sanidad, puede hacerlo a través de este for-

mulario, o presencialmente a través de la red de oficinas de asistencia en materia de registros utilizando este modelo de solicitud (versión editable e imprimible).

Asimismo, te asiste en todo momento el derecho para presentar una reclamación ante Agencia Española de Protección de Datos.

10. ¿Cómo protegemos tus datos?

Los Responsables, así como la SGAD en condición de encargada del tratamiento, garantizan la seguridad, el secreto y la confidencialidad de tus datos, comunicaciones e información personal y han adoptado las más exigentes y robustas medidas de seguridad y medios técnicos para evitar su pérdida, mal uso o su acceso sin tu autorización. Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Finalmente, te informamos que tanto el almacenamiento como el resto de las actividades del tratamiento de datos no personales utilizados estarán siempre ubicados dentro de la Unión Europea.

11. ¿Qué tienes que tener especialmente en cuenta al utilizar "Radar COVID"?

Has de tener en cuenta determinados aspectos relativos a la edad mínima de utilización de Aplicación, la calidad de los datos que nos proporcionas, así como la desinstalación de la Aplicación en tu dispositivo móvil.

Edad mínima de utilización: para poder utilizar “Radar COVID” tienes que ser mayor de 18 años o contar con la autorización de tus padres y/o tutores legales. Por tanto, al darte de alta en la Aplicación, garantizas al Titular que eres mayor de dicha edad o, en caso contrario, que cuentas con la mencionada autorización.

Calidad de los datos que nos proporcionas: la información que nos facilites en el uso de los servicios de la Aplicación deberá de ser siempre real, veraz y estar actualizada.

Desinstalación de la Aplicación: en general, puedes desinstalar la aplicación en tu dispositivo en cualquier momento. Este proceso elimina de tu teléfono móvil el historial de códigos recibidos desde otros teléfonos móviles para las funciones de alerta de contactos estrechos.

12. Transferencia de datos a países de la Unión Europea

Radar COVID participa en la plataforma de integración de aplicaciones de la unión europea, de manera que se compartirán las claves positivas con terceros países de la UE y viceversa.

Cuando el dispositivo del usuario descarga las claves positivas para analizar posibles contactos estrechos, descargará también las claves positivas de terceros países adheridos al proyecto europeo.

Esto permitirá identificar posibles contactos estrechos tanto si el usuario ha estado visitando alguno de estos países como si ha estado en contacto estrecho con un visitante procedente de estos países.

Cuando el usuario introduce un código de confirmación de diagnóstico positivo por COVID-19, se solicitará el consentimiento del usuario libre, específico, infor-

mado e inequívoco para compartir sus claves infectadas con terceros países a través de la plataforma de interoperabilidad europea facilitando el rastreo digital de posibles contactos estrechos. La comunicación de tus claves infectadas a la red de países europeos adheridos a este proyecto es completamente voluntaria.

No se efectuarán transferencias de datos fuera de la Unión Europea

13. Política de cookies

Utilizamos solamente cookies técnicas que permiten al usuario la navegación y la utilización de las diferentes opciones o servicios que se ofrecen en la Aplicación como, por ejemplo, acceder a partes de acceso restringido o utilizar elementos de seguridad durante la navegación.

He leído el documento POLÍTICA DE PRIVACIDAD DE LA APLICACIÓN "Radar COVID".

TRIGÉSIMO OCTAVO: En la versión final de las "Condiciones de Uso de Radar COVID" consta la siguiente información:

CONDICIONES DE USO DE Radar COVID

AL DESCARGAR Y USAR LA APLICACIÓN MÓVIL "Radar COVID" MANIFIESTAS QUE HAS LEÍDO Y ACEPTAS ESTAS CONDICIONES DE USO Y LA POLÍTICA DE PRIVACIDAD. AQUÍ SE RECOGE TODA LA INFORMACIÓN RELATIVA A TUS DERECHOS Y OBLIGACIONES COMO USUARIO DE ESTA APLICACIÓN.

AVISO IMPORTANTE:

El USUARIO queda avisado de que la utilización de la Aplicación NO CONSTITUYE EN NINGÚN CASO UN SERVICIO DE DIAGNÓSTICO MÉDICO, DE ATENCIÓN DE URGENCIAS O DE PRESCRIPCIÓN DE TRATAMIENTOS FARMACOLÓGICOS, pues la utilización de la Aplicación no podría en ningún caso sustituir la consulta presencial personal frente a un profesional médico debidamente cualificado.

1. Qué es Radar COVID

Radar COVID es una aplicación que promueve la salud pública mediante un sistema de alerta de contactos de riesgo en relación a la COVID-19, poniendo a disposición de los USUARIOS (en adelante, individualmente, el "USUARIO", y conjuntamente los "USUARIOS"), la posibilidad de navegar por la Aplicación, accediendo a los contenidos y servicios de Radar COVID, de acuerdo con las presentes CONDICIONES DE USO.

Radar COVID detecta la intensidad de señales Bluetooth intercambiadas entre dispositivos que tienen esta aplicación activa, mediante el empleo de identificadores aleatorios efímeros, que no guardan relación con la identidad del teléfono móvil empleado o el USUARIO. El dispositivo de cada USUARIO descarga periódicamente las claves Bluetooth de todos los USUARIOS de la aplicación que hayan informado a través de la misma que se les ha diagnosticado COVID-19 (previa acreditación de las autoridades sanitarias), procediendo a determinar si el USUARIO ha establecido contacto de riesgo con alguno de ellos, verificado por las señales Bluetooth intercambiadas. Si es el caso, la aplicación le notifica este hecho, a fin de que pueda para tomar medidas, y contribuir de este modo a

evitar que el virus se propague.

Radar COVID en su arquitectura emplea el Sistema de Notificación de Exposiciones (SNE) proporcionado por Apple y Google, y desarrollado a partir del Protocolo de DP-3T de rastreo de proximidad descentralizado para preservar la privacidad.

2. Uso de Radar COVID

Para la utilización de los servicios de Radar COVID, es requisito necesario que el USUARIO autorice la activación del sistema de comunicaciones Bluetooth de baja energía (BLE, Bluetooth Low Energy) por parte de la Aplicación, tras la descarga de la misma.

El USUARIO acepta sin reserva el contenido de las presentes CONDICIONES DE USO. En consecuencia, el USUARIO deberá leer detenidamente las mismas antes del acceso y de la utilización de cualquier servicio de Radar COVID bajo su entera responsabilidad.

AVISO IMPORTANTE: La utilización de la Aplicación es gratuita, libre y voluntaria para todos los ciudadanos. Para utilizar Radar COVID no es necesario estar registrado, ni aportar ningún dato personal, identificativo o no identificativo. Al activar la aplicación, el USUARIO acepta:

a) envío de señales Bluetooth emitidas de forma anónima por su dispositivo;

b) la recepción y almacenamiento de señales Bluetooth de aplicaciones compatibles con Radar COVID, que se mantienen de forma anónima y descentralizada en los dispositivos de los USUARIOS durante un periodo no superior a 14 días;

c) la información ofrecida al USUARIO sobre el posible riesgo de contagio, sin que en ningún momento se refieran datos personales de ningún tipo.

d) recibir claves positivas de terceros países de la Unión Europea a través de la plataforma de interoperabilidad de la unión europea (EFGS);

e) bajo consentimiento explícito, el envío de claves positivas que serán compartidas con terceros países de la Unión Europea a través de la plataforma de interoperabilidad de la unión europea (EFGS).

El USUARIO puede informar voluntariamente a la aplicación de un resultado positivo en sus pruebas de COVID-19 mediante el código de confirmación de un solo uso facilitado por las autoridades sanitarias. La validez de este código será cotejada por la aplicación para asegurar el correcto funcionamiento de Radar COVID. El USUARIO informará de los resultados de sus pruebas y se le solicitará el consentimiento expreso e inequívoco para compartir las claves generadas diariamente en su dispositivo, y correspondientes a los últimos 14 días. Estas claves son comunicadas a un servidor que las pondrá a disposición del conjunto de aplicaciones Radar COVID para su descarga. Las claves comunicadas no guardan relación alguna con la identificación del dispositivo o el USUARIO.

3. Seguridad y privacidad

Las medidas de seguridad implantadas se corresponden con las previstas en el anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

Te informamos que tus datos serán tratados conforme a lo establecido en la Política de Privacidad de la Aplicación, cuyo contenido íntegro se puede consultar en el siguiente enlace: Política de Privacidad.

Toda la información se tratará con fines estrictamente de interés público en el ámbito de la salud pública, y ante la situación de emergencia sanitaria decretada, a fin de proteger y salvaguardar un interés esencial para la vida de las personas, en los términos descritos en la política de privacidad.

La información de la actividad de los USUARIOS es anónima y en ningún momento se exigirá a los USUARIOS ningún dato personal. En todo momento, el USUARIO puede desactivar el sistema de traza de contactos Bluetooth en la aplicación, así como desinstalar la Aplicación.

4. Cambio del servicio y terminación

Radar COVID siempre está tratando de mejorar el servicio y busca ofrecer funcionalidades adicionales útiles para el USUARIO teniendo siempre presente la preservación de la salud pública. Esto significa que podemos añadir nuevas funciones o mejoras, así como eliminar algunas de las funciones. Si estas nuevas funciones o mejoras afectan materialmente a los derechos y obligaciones del USUARIO, será informado a través de la Aplicación para que adopte las decisiones oportunas sobre la continuación de su uso.

El USUARIO puede dejar de utilizar la aplicación en cualquier momento y por cualquier motivo, desinstalándola de su dispositivo.

5. Titular de la aplicación

La Secretaría General de Administración Digital (SGAD), dependiente de la Secretaría de Estado de Digitalización e Inteligencia Artificial del Ministerio de Asuntos Económicos y Transformación Digital, es el órgano TITULAR de la aplicación.

6. Responsabilidad y obligaciones

Radar COVID se ofrece dedicando los mejores esfuerzos, dado que su calidad y disponibilidad pueden verse afectadas por múltiples factores ajenos al TITULAR como son, entre otros, el volumen de otros USUARIOS en la ubicación geográfica del USUARIO, limitaciones o restricciones de las redes de terceros operadores o la compatibilidad del dispositivo y sistema operativo utilizado por el USUARIO. Igualmente, los USUARIOS aceptan que el servicio pueda verse interrumpido cuando sea necesario por labores de mantenimiento.

Por todo ello, el TITULAR no será responsable de los problemas de acceso o disponibilidad de Radar COVID y/o de sus servicios, ni de los perjuicios que se pudieran causar por ello, cuando éstos procedan de factores ajenos a su ámbito de control.

Igualmente, el TITULAR no se hace responsable de los siguientes hechos, ni de fallos, incompatibilidades y/o daños de tus terminales o dispositivos que, en su caso, se pudiesen derivar de la descarga y/o uso de la Aplicación:

Actualización, exactitud, exhaustividad, pertinencia, actualidad y fiabilidad de sus contenidos, cualquiera que sea la causa y las dificultades o problemas técnicos o de otra naturaleza en los que tengan su origen dichos hechos.

La calidad, titularidad, legitimidad, adecuación o pertinencia de los materiales, y demás contenidos.

Como USUARIO de la Aplicación te obligas a:

Impedir el acceso de terceras personas no autorizadas a la aplicación desde tu dispositivo.

Notificar al TITULAR con carácter inmediato cualquier indicio de la existencia de una violación en la seguridad en la Aplicación, de usos inapropiados o prohibidos de los servicios prestados desde la misma, o de fallos de seguridad de cualquier índole.

Hacer buen uso de los contenidos, información y servicios prestados desde o a través de la Aplicación, conforme a la ley, la buena fe y a las buenas costumbres generalmente aceptadas, comprometiéndose expresamente a:

Abstenerse de realizar prácticas o usos de los servicios con fines ilícitos, fraudulentos, lesivos de derechos o intereses del TITULAR o de terceros, infractores de las normas contenidas en el presente documento.

Abstenerse de realizar cualquier tipo de acción que pudiera inutilizar, sobrecargar o dañar sistemas, equipos o servicios de la Aplicación o accesibles directa o indirectamente a través de esta.

Respetar los derechos de propiedad intelectual e industrial del TITULAR y de terceros sobre los contenidos, información y servicios prestados desde o a través de la Aplicación, absteniéndose con carácter general de copiar, distribuir, reproducir o comunicar en forma alguna los mismos a terceros, de no mediar autorización expresa y por escrito del TITULAR o de los titulares de dichos derechos.

No proporcionar información falsa en la Aplicación, siendo el único responsable de la comunicación real y veraz.

No suplantar la personalidad de un tercero.

El USUARIO de la Aplicación es el único responsable del uso que decida realizar de los servicios de Radar COVID.

El TITULAR no será responsable en ningún caso de la utilización indebida de Radar COVID y de sus contenidos, siendo el USUARIO el único responsable por los daños y perjuicios que pudieran derivarse de un mal uso de estos o de la infracción de lo dispuesto en las presentes condiciones en que pueda incurrir. El USUARIO se compromete a mantener indemne al TITULAR frente a las reclamaciones o sanciones que pudiera recibir de terceros, ya sean particulares o entidades públicas o privadas, por razón de dichas infracciones, así como frente a los daños y perjuicios de todo tipo que pueda sufrir como consecuencia de las mismas.

En cualquier caso, el TITULAR se reserva, en cualquier momento y sin necesidad de previo aviso, el derecho de modificar o eliminar el contenido, estructura, diseño, servicios y condiciones de acceso y/o uso de esta Aplicación, siempre que dicho cambio no afecte a los principios y derechos de protección de datos, así como el derecho interpretar las presentes condiciones, en cuantas cuestiones pudiera plantear su aplicación.

Asimismo, queda prohibida la reproducción, distribución, transmisión, adaptación

o modificación, por cualquier medio y en cualquier forma, de los contenidos de Radar COVID o sus cursos (textos, diseños, gráficos, informaciones, bases de datos, archivos de sonido y/o imagen, logos y demás elementos de estos sitios), salvo las permitidas por la licencia de liberación de código abierto bajo la que se ha publicado el sistema.

La enumeración anterior tiene mero carácter enunciativo y no es, en ningún caso, exclusivo ni excluyente en ninguno de sus puntos. En todos los supuestos, El TITULAR EXCLUYE CUALQUIER RESPONSABILIDAD POR LOS DAÑOS Y PERJUICIOS DE CUALQUIER NATURALEZA DERIVADOS DIRECTA O INDIRECTAMENTE DE LOS MISMOS Y DE CUALESQUIERA OTROS NO ESPECIFICADOS DE ANÁLOGAS CARACTERISTICAS.

El TITULAR NO OFRECE NINGUNA GARANTÍA, EXPRESA, IMPLÍCITA, LEGAL O VOLUNTARIA.

EL TITULAR EXCLUYE EXPRESAMENTE TODAS LAS GARANTÍAS IMPLÍCITAS, INCLUYENDO, A TÍTULO ENUNCIATIVO, PERO NO LIMITATIVO, CUALQUIER GARANTÍA IMPLÍCITA O SANEAMIENTO DE VICIOS OCULTOS, COMERCIABILIDAD, CALIDAD SATISFACTORIA, TÍTULO, IDONEIDAD DEL PRODUCTO PARA UN PROPÓSITO EN PARTICULAR Y CUALQUIER GARANTÍA O CONDICIÓN DE NO INFRACCIÓN. ESTA EXCLUSIÓN DE RESPONSABILIDAD SÓLO SE APLICARÁ EN LA MEDIDA PERMITIDA POR LA LEY IMPERATIVA APLICABLE.

7. Enlaces

Radar COVID puede incluir dentro de sus contenidos enlaces con sitios pertenecientes y/o gestionados por terceros con el objeto de facilitar el acceso a información y servicios disponibles a través de Internet.

El TITULAR no asume ninguna responsabilidad derivada de la existencia de enlaces entre los contenidos de Radar COVID y contenidos situados fuera de los mismos o de cualquier otra mención de contenidos externos, exceptuando aquellas responsabilidades establecidas en la normativa de protección de datos. Tales enlaces o menciones tienen una finalidad exclusivamente informativa y, en ningún caso, implican el apoyo, aprobación, comercialización o relación alguna entre el TITULAR y las personas o entidades autoras y/o gestoras de tales contenidos o titulares de los sitios donde se encuentren, ni garantía alguna del TITULAR por el correcto funcionamiento de los sitios o contenidos enlazados.

En este sentido el USUARIO se obliga a poner la máxima diligencia y prudencia en el caso de acceder o usar contenidos o servicios de los sitios a los que acceda en virtud de los mencionados enlaces.

8. Hiperenlaces

No se admite la reproducción de páginas de Radar COVID mediante hiperenlace desde otra Aplicación móvil o página web, permitiéndose exclusivamente el acceso desde la Aplicación.

En ningún caso se podrá dar a entender que el TITULAR autoriza el hiperenlace o que ha supervisado o asumido de cualquier forma los servicios o contenidos ofrecidos por la web desde la que se produce el hiperenlace.

No se podrán realizar manifestaciones o referencias falsas, incorrectas o inexac-

tas sobre las páginas y servicios del TITULAR.

Se prohíbe explícitamente la creación de cualquier tipo de navegador, programa, "browser" o "border environment" sobre las páginas de Radar COVID.

No se podrán incluir contenidos contrarios a los derechos de terceros, ni contrarios a la moral y las buenas costumbres aceptadas, ni contenidos o informaciones ilícitas, en la página web desde la que se establezca el hiperenlace.

La existencia de un hiperenlace entre una página web y el Radar COVID no implica la existencia de relaciones entre el TITULAR y el propietario de esa página, ni la aceptación y aprobación de sus contenidos y servicios.

9. Ley aplicable y fuero

Las presentes condiciones de uso se regirán e interpretarán en todos y cada uno de sus extremos por la legislación española. En aquellos casos en los que la normativa vigente no prevea la obligación de someterse a un fuero o legislación determinado, el TITULAR y los USUARIOS, con renuncia a cualquier otro fuero que pudiera corresponderles, se someten a los juzgados y tribunales de Madrid capital (España).

10. Información corporativa y contacto

Dirección: Calle de Manuel Cortina, 2, 28010 Madrid

TRIGÉSIMO NOVENO: Con fecha 15 de octubre de 2020 se publica en el BOE la "Resolución de 13 de octubre de 2020, de la Subsecretaría, por la que se publica el Acuerdo entre el Ministerio de Asuntos Económicos y Transformación Digital y el Ministerio de Sanidad, acerca de la aplicación "Radar COVID"". Con fecha 10/10/2020 entra en vigor dicha resolución.

El Acuerdo se suscribe entre el Secretario General de Administración Digital, por delegación de la SEDIA, y el Secretario General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, por delegación del MSND.

En este se señalan las competencias de los intervinientes:

"Segundo.- Que de acuerdo con lo previsto en el artículo 7.1 del Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud (en adelante, SGSDII) es el órgano directivo del Ministerio de Sanidad al que, bajo la superior dirección de la persona titular del Departamento, corresponde abordar los proyectos de modernización, innovación, mejora y transformación del Sistema Nacional de Salud.

Tercero. Que, de acuerdo con lo previsto en el artículo 8.2.a) del Real Decreto 735/2020, de 4 de agosto, la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud es el órgano directivo dependiente de la Secretaría General de Salud Digital a quien corresponde el diseño, desarrollo e implantación de los servicios electrónicos comunes del Sistema Nacional de Salud, las aplicaciones informáticas y de salud digital del Ministerio de Sanidad, así como los portales sectoriales y horizontales de dicho Departamento, garantizando su integración y homogeneidad

Cuarto.- Que de acuerdo con lo previsto en el Real Decreto 403/2020, de 25 de febrero, por el que se desarrolla la estructura orgánica básica del Ministerio de Asuntos Económicos y Transformación Digital, corresponde a la Secretaría General de Administración Digital (en adelante SGAD), órgano directivo de la Secretaría de Estado de Digitalización e Inteligencia Artificial, la dirección, coordinación y ejecución de las competencias atribuidas a la Secretaría de Estado en materia de transformación digital de la administración".

En el "EXPONEN" Sexto dice:

"Que en aplicación de dichos principios, desde el mes de mayo de 2020, la SGAD ha venido desarrollando, con el conocimiento y la conformidad del Ministerio de Sanidad, una aplicación para la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 denominada «Radar COVID. Durante el mes de julio de 2020, con la conformidad de la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, la SGAD llevó a cabo con éxito el proyecto piloto de la misma, cuyo éxito garantiza la viabilidad de la solución propuesta para el rastreo de contactos estrechos"

En el "EXPONEN" Noveno dice:

"Que, hasta el momento, el Ministerio de Sanidad ha venido colaborando con la SGAD, titular de la aplicación «Radar COVID», en los procesos de ajuste funcional de la misma desde la perspectiva de salud pública, coordinando los protocolos de manejo epidemiológico de casos detectados a través de la aplicación, y favoreciendo la incorporación progresiva de las comunidades y ciudades autónomas a su utilización en fase de pruebas con datos reales según el mencionado Acuerdo de 19 de agosto de 2020."

La primera de las cláusulas dice:

Primera. Objeto. Es objeto del presente Acuerdo:

a) Delegar en la Secretaría General de Administración Digital (en adelante, SGAD) del Ministerio de Asuntos Económicos y Transformación Digital, todas las competencias de diseño, desarrollo, implantación y evolución de la aplicación «Radar COVID» que correspondan a la Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud en virtud de lo previsto en el artículo 8.2.a) del Real Decreto 735/2020, de 4 de agosto, por el que se desarrolla la estructura orgánica básica del Ministerio de Sanidad, la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud. La Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud ha aprobado previamente la delegación de todas estas competencias en la SGAD de acuerdo con lo previsto en el artículo 9.1 de la Ley 40/2015, de 1 de octubre.

b) Delegar en la SGAD la competencia del Ministro de Sanidad para suscribir con las comunidades y ciudades autónomas los convenios de colaboración para la adhesión de estas al uso de la aplicación «Radar COVID», de acuerdo con lo previsto en el Capítulo VI del Título Preliminar de la Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. sin perjuicio del apoyo que para facilitar su tramitación le prestará la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud.

La segunda de las cláusulas dice:

Segunda. Obligaciones de las partes con relación a la delegación de competencias prevista en la letra a) de la cláusula primera:

1. Con la firma del presente Acuerdo, con relación a la delegación de competencias prevista en la letra a) de la cláusula primera la SGAD se compromete al cumplimiento de las siguientes obligaciones:

a) La contratación del mantenimiento evolutivo, correctivo, adaptativo y perfectivo del sistema «Radar COVID» con cargo a sus créditos presupuestarios.

b) La publicación en abierto del código fuente del sistema «Radar COVID».

c) El soporte a la operación del sistema y la gestión de la infraestructura asociada.

d) El soporte y atención a usuarios y comunidades y ciudades autónomas en relación con los aspectos técnicos de este sistema.

e) Cualesquiera otras obligaciones necesarias para el correcto funcionamiento de la aplicación y, en especial su integración con el sistema europeo de intercambio de contactos, incluyendo la solicitud formal de adhesión al sistema.

2. Las decisiones en relación con la evolución de la Aplicación se adoptarán de común acuerdo entre las partes.

3. Con relación a la delegación de competencias prevista en la letra a) de la cláusula primera de este Acuerdo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, además de sus obligaciones como Responsable del tratamiento de datos de carácter personal, y su Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud, las siguientes obligaciones:

a) El seguimiento del diseño e implementación del sistema «Radar COVID».

b) La recepción de los datos que obren en poder de la SGAD (relacionados con su descarga activa, uso, códigos utilizados, etc) para el adecuado seguimiento epidemiológico de la Pandemia en España, así como su relación con otros países europeos.

c) El impulso de las medidas necesarias para su correcta aplicación dentro del ámbito de competencias de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, así como el impulso de los acuerdos que fuera necesario adoptar al respecto en el Consejo Interterritorial del Sistema Nacional de Salud.

d) El análisis del cumplimiento de objetivos y, en su caso, la propuesta de reformulación de procedimientos e indicadores para ajustarlos a necesidades sobrevenidas.

e) Cualesquiera otras obligaciones necesarias para el correcto funcionamiento de la aplicación.

La tercera de las cláusulas en el apartado 1 y 2 dice:

1. En los Convenios de colaboración que la SGAD subscriba por delegación del Ministro de Sanidad para la adhesión de las comunidades y ciudades autónomas al uso de la aplicación «Radar COVID», la SGAD se comprometerá al cumplimiento de las siguientes obligaciones:

a) La puesta a disposición del uso de la Aplicación conforme a lo previsto en el Convenio.

b) La distribución a las consejerías competentes en materia de sanidad de los códigos positivos necesarios para que los usuarios de la Aplicación con test PCR positivo los introduzcan en la misma, garantizando así la inexistencia de falsos positivos en el sistema.

c) La adopción de las medidas de seguridad precisas para proteger la información contenida en la aplicación y los sistemas asociados a soluciones tecnológicas objeto de dicho Convenio.

d) La asunción del compromiso de no reidentificación de los interesados.

e) La asunción del compromiso de no almacenamiento de códigos o elementos que pudieran llegar a permitir la reidentificación de las personas, incluyendo direcciones IP.

f) El establecimiento de plazos de limitación y supresión de las informaciones obtenidas, incluidos los logs del aplicativo, como parte del ciclo de vida del dato, previa aprobación del Ministerio de Sanidad en su condición de responsable del tratamiento.

g) La asunción del compromiso de no llevar a cabo el procesamiento unilateral de los datos, dando lugar a tratamientos u operaciones de tratamiento diferentes a las establecidas en el convenio o similares que no hubieran sido previstas en dicho convenio.

h) La asunción del compromiso de no llevar a cabo la toma de decisiones automatizadas u otras decisiones que pudieran afectar a los interesados.

i) El establecimiento, junto con la consejería competente en materia de sanidad de la comunidad o ciudad autónoma de que se trate, del detalle de quién pone fin al ciclo de vida del tratamiento de datos personales y términos en los que debería llevarse a cabo la eliminación definitiva de toda información, junto con el compromiso de ambas partes de no mantener datos más allá del acuerdo del fin del ciclo de vida del tratamiento.

j) Cualesquiera otras obligaciones necesarias para el buen fin de la aplicación que la SGAD pueda llevar a cabo en su ámbito competencial.

2. En los mencionados Convenios de colaboración, el Ministerio de Sanidad y la Consejería competente en materia de sanidad de la comunidad o ciudad autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y la SGAD como encargado del tratamiento, a los efectos previstos en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo de 27 de abril de 2016 relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) y en la Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales y demás normativa de aplicación en materia de protección de datos.

3. Con relación a la delegación de competencias prevista en la letra b) de la cláusula primera de este Acuerdo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, en su

<u>condición de Responsable del tratamiento de datos de carácter personal, dar las indicaciones necesarias a la SGAD en su condición de encargado del tratamiento.</u>

Asimismo, corresponden a la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud y su Dirección General de Salud Digital y Sistemas de Información para el Sistema Nacional de Salud las siguientes obligaciones:

a) La colaboración con la SGAD y las consejerías de las comunidades y ciudades autónomas competentes en la materia en todas las acciones necesarias para la correcta implantación y desarrollo del sistema «Radar COVID».

b) Velar por el correcto funcionamiento del sistema «Radar COVID», en particular en lo referente a la defensa de los derechos de los interesados.

c) El seguimiento permanente de los resultados del sistema «Radar COVID» para trasladarlos a las autoridades sanitarias de las distintas Administraciones Públicas.

d) El impulso de las medidas necesarias para su correcta desarrollo y ejecución dentro del ámbito de competencias de la Secretaría General de Salud Digital, Información e Innovación del Sistema Nacional de Salud, así como el impulso de los acuerdos que fuera necesario adoptar al respecto en el Consejo Interterritorial del Sistema Nacional de Salud.

e) Cualesquiera otras obligaciones necesarias para el buen fin de la aplicación que puedan abordarse desde las competencias de la dicha Secretaría General.

La cláusula décima dice:

Décima. Régimen de protección de datos, seguridad y confidencialidad.

1. El régimen de protección de datos de carácter personal en las actuaciones que se desarrollen en ejecución del presente Acuerdo será el previsto en el Reglamento general de protección de datos y en la Ley Orgánica 3/2018, de 5 de diciembre, y demás normativa de aplicación en materia de protección de datos.

2. Las partes velarán por el cumplimiento del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

3. Toda la información facilitada por las partes y toda la información generada como consecuencia de la ejecución del presente Acuerdo, tendrá el tratamiento de confidencial, sin perjuicio de la información que sea de dominio público, no pudiendo ser divulgada o facilitada a terceros, ni utilizada para un fin distinto del previsto en este documento, sin el acuerdo unánime de las partes.

4. La obligación de confidencialidad para las partes se extenderá indefinidamente aunque el Acuerdo se hubiera extinguido. Todo ello sin perjuicio de la eventual autorización de las partes o en su caso, de que dicha información pasara a ser considerada como de dominio público.

<u>CUADRAGÉSIMO</u>: Con fecha 22 de octubre de 2020 el METD publica esta nota de prensa:
"Las principales operadoras de telefonía se comprometen a no repercutir el consumo de datos de la app RadarCOVID a sus usuarios. (…)

La secretaria de Estado de Digitalización e Inteligencia Artificial, Carme Artigas, ha mantenido esta mañana un encuentro con representantes de las principales operadoras de telefonía del país con el objetivo de establecer vías de colaboración para la difusión de la aplicación móvil de traceo de contactos RadarCOVID.

La reunión se enmarca dentro de una serie de encuentros sectoriales con distintos actores, instituciones y empresas para explorar posibles modelos de apoyo para la expansión e implantación entre la ciudadanía de esta herramienta digital."

CUADRAGÉSIMO PRIMERO: La App Radar COVID consta inscrita en el Registro de actividades de tratamiento (RAT) del MSND, SGSDII, en los siguientes términos:

RESPONSABLE:

SECRETARÍA GENERAL DE SALUD DIGITAL, INFORMACIÓN E INNOVACIÓN DEL SISTEMA NACIONAL DE SALUD. Paseo del Prado, 18. 20. Madrid 28071. sgsdii@sanidad.gob.es

DELEGADA DE PROTECCION DE DATOS Titular de la Inspección General de Servicios del Ministerio. delegadoprotecciondatos@mscbs.es

FINES DEL TRATAMIENTO:

El tratamiento tiene por finalidad facilitar la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 mediante alertas al usuario.

BASE JURÍDICA DEL TRATAMIENTO:

• Interés público esencial en el ámbito específico de la salud pública, y para la protección de intereses vitales de los afectados y de otras personas físicas al amparo de lo establecido en el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016.

• Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.

• Ley 14/1986, de 25 de abril, General de Sanidad

•Ley Orgánica 3/1986, de 14 de abril, de Medidas Especiales en Materia de Salud Pública.

• Ley 33/2011, de 4 de octubre, General de Salud Pública.

• Real Decreto 463/2020 de 14 de marzo, por el que se declara el estado de alarma para la gestión de la situación de crisis sanitaria ocasionada por el COVID.19 que atribuye al Ministro de Sanidad la necesaria competencia en todo el territorio nacional.

• Orden Ministerial SND/297/2020 de 27 de marzo, por la que se encomienda a la Secretaría de Estado de Digitalización e Inteligencia Artificial, del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de nuevas actuaciones.

CATEGORIAS DE INTERESADOS

Personas que voluntariamente se han descargado la aplicación móvil, han sido

diagnosticadas como caso positivo en COVID y han remitido el código facilitado por los servicios de salud de las CCAAs en la aplicación.

CATEGORIAS DE DATOS PERSONALES:

Los datos manejados por la aplicación no permiten la identificación directa del usuario o de su dispositivo ni su geolocalización.

Como parte del sistema de alerta de contagios de la COVID-19, se procesarán los siguientes datos para los usuarios que hayan dado positivo por COVID.19 para los fines especificados a continuación:

o Las claves de exposición temporal con las que el dispositivo del usuario ha generado los códigos aleatorios enviados (identificadores efímeros Bluetooth), a los dispositivos con los que el usuario ha entrado en contacto, hasta un máximo de 14 días anteriores.

o Un código de confirmación de un solo uso de 12 dígitos facilitado por las autoridades sanitarias en caso de prueba positiva por COVID.19.

Cuestionario voluntario para la recogida de información sobre la experiencia de uso de la aplicación, comprensión de la misma o percepción sobre la privacidad, entre otros.

CATEGORIAS DE DESTINATARIOS:

Usuario de la aplicación.

TRANSFERENCIAS INTERNACIONALES:

No previstas, salvo obligación legal.

PLAZO DE SUPRESIÓN

Las claves de exposición temporal y los identificadores efímeros de Bluetooth son almacenados en el dispositivo por un periodo de 14 días, después de los cuales son eliminados.

Asimismo, las claves de exposición temporal que hayan sido comunicadas al servidor por los USUARIOS diagnosticados como positivos por COVID-19 también serán eliminadas del servidor al cabo de 14 días.

MEDIDAS TECNICAS Y ORGANIZATIVAS DE SEGURIDAD:

Las medidas de seguridad implantadas se corresponden con las previstas en el Anexo II (Medidas de seguridad) del Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica y que se encuentran descritas en los documentos que conforman la Política de protección de datos y seguridad de la información del Ministerio.

CUADRAGÉSIMO SEGUNDO: No consta acreditado que la SEDIA recabara el asesoramiento del delegado de protección de datos del METD, al realizar la evaluación de impacto relativa a la protección de datos.

CUADRAGÉSIMO TERCERO: Con fecha 9 de septiembre de 2020 se produce la publicación en abierto del código fuente del sistema «Radar COVID»:

radar-covid-android – Aplicación RadarCOVID para Android - 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-android at 67a4506cc43a20062e87aebd5caa6-

be2ea0f6482

radar-covid-ios – Aplicación iOS para RadarCOVID – 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-ios at 118d6239fc42e369db83e0f2555b62d3e72fc1be

radar-covid-backend-dp3t-server – Servidor DPT3 - 9 Sept 2020 – GitHub - RadarCOVID/radar-covid-backend-dp3t-server at 2ea39a5e03ad3da1ff4c7f6567be6b778fb79c7d

CUADRAGÉSIMO CUARTO: En el escrito de respuesta al requerimiento de fecha 26 de octubre de 2020, notificado a la SEDIA, se confirma la existencia de una vulnerabilidad que es corregida en la subida correspondiente al 8 de octubre, para las siguientes versiones de la aplicación:

1. Android, versión 1.0.9

2. Apple, versión 1.0.8

Se confirma que a fecha de 8 de octubre, se habían declarado un total de 3.059 códigos a nivel nacional, si bien es cierto que a fecha de la publicación del código fuente (9/sep), ya se habían reportado un total de 574 códigos.

CUADRAGÉSIMO QUINTO: En enero de 2022 se continua facilitando la siguiente información en las "Preguntas frecuentes" del sitio web: https://radarcovid.gob.es/faq-datos-personales-y-privacidad:

¿Cómo se protege mi privacidad?

Durante todo el proceso de diseño y desarrollo de Radar COVID, la protección de tu privacidad ha sido una prioridad.

Aquí tienes una lista de algunas de las medidas con las que Radar COVID protege tus datos:

- *La aplicación no recopila ningún dato que permita rastrear tu identidad. Por ejemplo, no te preguntará y no podrá conocer tu nombre, apellidos, dirección, número de teléfono o dirección de correo electrónico.*
- *La aplicación no recopila ningún dato de geolocalización, incluidos los del GPS. Además, tampoco realiza ningún seguimiento de tus desplazamientos.*
- *El código de Bluetooth Low Energy (de baja energía) que se transmite a través de la aplicación se genera aleatoriamente y no contiene ninguna información sobre tu smartphone ni sobre ti.*
- *Además, este código cambia varias veces cada hora para proteger aún más tu privacidad.*
- *Los datos que se guardan en tu teléfono móvil están cifrados.*
- *Las conexiones entre la aplicación y el servidor están cifradas.*
- *Todos los datos, tanto los que se guardan en el dispositivo (códigos intercambiados con otros teléfonos móviles) son eliminados al cabo de 14 días.*
- *Asimismo, los datos recogidos en el servidor, procedentes de los teléfonos móviles donde se ha reportado un diagnóstico positivo por COVID-19, son eliminados al cabo de 14 días.*
- *Ningún dato almacenado en los teléfonos móviles o en el servidor permi-*

te la identificación ni del propio dispositivo móvil ni del usuario del mismo

¿Radar COVID comparte o vende mis datos?

Radar COVID no recoge datos personales de ningún tipo. Solo almacena en los dispositivos móviles información sobre los códigos provenientes de otros teléfonos móviles que han estado en proximidad con tu teléfono. Estos códigos no permiten identificar ni al dispositivo ni a su usuario.

El servidor con el que se comunican las aplicaciones en caso de reportarse un diagnóstico positivo por la COVID-19, solo almacena los códigos que ha generado el teléfono de la persona infectada, en los últimos 14 días. De nuevo, estos códigos son aleatorios y no permiten identificar ni al dispositivo móvil ni al usuario.

Por todo lo anterior, Radar COVID no maneja información susceptible de ser vendida o utilizada para ningún objetivo comercial, incluyendo la creación de perfiles con fines publicitarios. Este proyecto no tiene ningún ánimo de lucro, siendo creado exclusivamente para ayudar a combatir la epidemia. No se descarta el análisis de datos agregados sobre volumen de descargas de la aplicación, volumen de usuarios contagiados, u otros indicadores anónimos y agregados, para proyectos de investigación científica.

TERCERO: La SEDIA ha presentado en fecha 28 de marzo de 2022, ante el Registro General de la AEPD, recurso potestativo de reposición en el que, tras exponer una serie de antecedentes, da por reproducidas todas las alegaciones efectuadas a lo largo de la tramitación del expediente, así como toda la documentación remitida en el periodo de prueba y durante el periodo de información reservada.

Asimismo, muestra su disconformidad con la resolución impugnada e invoca -en síntesis- una serie de argumentos expuestos a continuación:

I

Considera que no se ha producido el incumplimiento de los artículos que se señalan en base a los siguientes argumentos:

II

Alude a reflexionar sobre el contexto jurídico y social en el que se desarrolla la aplicación que condiciona de forma sustancial todas las actuaciones practicadas y los roles de todos los agentes que participaron en su desarrollo.

Así, de acuerdo con lo previsto en el artículo 4 del Real Decreto 463/2020, se designaron como autoridades competentes delegadas, bajo la superior dirección del Presidente del Gobierno, entre otras, al Ministro de Sanidad. Los Ministros designados, estaban habilitados para dictar las órdenes, resoluciones, disposiciones e instrucciones interpretativas que, en la esfera específica de su actuación, fueran necesarios para garantizar la prestación de todos los servicios, ordinarios o extraordinarios, en orden a la protección de personas, bienes y lugares. Una Instrucción u Orden de una Autoridad delegada del Gobierno, cobra bajo una situación de estado de alarma, una dimensión y fuerza muy su-

perior al que podría tener o desplegar si no se diera esta circunstancia.

En este contexto, la SEDIA, actuó conforme a las indicaciones dadas en todo momento por el MSND, como autoridad delegada del Gobierno en materia de Sanidad y en materia de salud pública, y como autoridad responsable del tratamiento de la aplicación Radar Covid.

Es cierto que estas indicaciones no se plasmaron en un contrato tal como se prevé en el artículo 28.1 a) del RGPD y ello es así, porque el estado de alarma dificultó la formalización de los instrumentos habituales previstos en la legislación para estos supuestos en circunstancias normales.

Sí está acreditada, en la documentación aportada en el periodo de prueba, la celebración de una serie de reuniones a las que asistieron representantes del MSND, de la SEDIA y de la empresa adjudicataria del contrato de emergencia para el desarrollo del piloto y de la aplicación Radar Covid, en las que se tomaban las decisiones necesarias de forma conjunta para avanzar en el desarrollo del piloto y de la aplicación.

La declaración del Estado de alarma y de la emergencia sanitaria, la protección de la salud en un contexto de pandemia determinó la necesidad de actuar rápidamente de forma coordinada con la colaboración de todos los agentes implicados y la relación entre responsable y encargado de tratamiento se produjo de una manera más ágil, tal como exigían las circunstancias.

Además, el METD a través de la SGAD dependiente de la SEDIA, como encargado del tratamiento, mantuvo contactos muy frecuentes con el MSND, para recibir sus indicaciones y estar ambos departamentos alineados en la consecución del objetivo común.

La SEDIA actuó siempre movida por razones de interés público y siguiendo las indicaciones del Gobierno y sus autoridad delegada (el Ministro de Sanidad de acuerdo con el Real Decreto 463/2020, de 14 de marzo) para ayudar a atajar la emergencia.

III

La AEPD distingue, en la Resolución sancionadora 2 etapas diferenciadas:

1º. La etapa en la que se hace el proyecto piloto

El 9 de junio de 2020 la SEDIA recibió el visto bueno de la DGSP del MSND para conducir un proyecto piloto en la isla de la Gomera, lo que posibilitó la realización del correspondiente expediente de contratación, con una duración de cinco meses, hasta el 14 de noviembre de 2020.

Aduce que, la SEDIA quedó como encargada del tratamiento a pesar de que su rol no se recogiera de forma explícita en la carta de 9 de junio.

Alude a la aplicación ASISTENCIA COVID, que supuso la primera colaboración de la SEDIA con el MSND en la lucha contra la pandemia, en la que el rol de-

sempeñado por la SEDIA fue también el de encargada de tratamiento.

Tanto el MSND, a través de la DGSP, como las autoridades sanitarias del Gobierno de Canarias participaron en las reuniones semanales del piloto para la conformación de los fines y medios del proyecto.

En todo caso, los datos que se manejaron en el piloto realizado entre los meses de junio y julio de 2020 eran datos simulados de infección (datos no reales), no poniéndose en compromiso ningún dato relacionado con la salud de los participantes en el piloto.

2º.- La etapa en la que se pone en marcha la aplicación en fase de pruebas y posteriormente la aplicación definitiva.

Alude al apartado 5 del Acuerdo adoptado el 19 de agosto de 2020 en el Consejo Interterritorial del Sistema Nacional de Salud que se refiere a la SEDIA como encargada del tratamiento y que permitió que las CCAA pudieran asumir temporalmente, hasta la firma de los convenios, la gestión de los códigos de diagnóstico positivo que se asignasen a aquellos ciudadanos con una prueba diagnóstica positiva de infección activa (PCR u otras técnicas). También a la hoja de ruta para hacer frente al ascenso de la "segunda curva epidemiológica" presentada por el presidente del Gobierno en la que se citó, entro otras medidas, el refuerzo de los medios digitales de rastreo.

Asimismo alude a la Resolución de 13 de octubre de 2020, en la que se refiere a la SGAD como encargada del tratamiento y a los diferentes Convenios celebrados entre la SGAD y las CCAA, donde se dispone que corresponde a la SGAD, entre otras funciones, cumplir con los cometidos como encargada del tratamiento indicado por el MSND como responsable del mismo.

Por tanto, según la SEDIA queda plenamente acreditado que en todo momento y de acuerdo con los instrumentos jurídicamente vinculantes, la SGAD actuó y actúa única y exclusivamente como encargada del tratamiento, mientras que el MSND y CCAA eran y son las responsables de dicho tratamiento.

En tal sentido, Radar Covid ha sido elaborada siguiendo los criterios epidemiológicos de la "Estrategia de detección precoz, vigilancia y control del COVID-19"2 publicada por el MSND y este departamento, ha facilitado directrices a la SEDIA-SGAD, como por ejemplo las recogidas en el documento técnico denominado "Procedimiento de implementación de la App Radar Covid como complemento a los sistemas manuales de identificación de contactos", coordinado por el Centro de Coordinación de Alertas y Emergencias Sanitarias, Dirección General de Salud Pública, Calidad e Innovación y aprobado por la Ponencia de Alertas y Planes de Preparación y Respuesta.

En todo momento, tanto en el desarrollo del piloto en la Isla de la Gomera, como en el uso de Radar Covid en pruebas por las Comunidades Autónomas, y en su uso superada dicha fase de pruebas, estaban definidos los roles de responsable de tratamiento y de encargado de tratamiento, por lo que, no pueden existir dudas de la legitimación que cada uno tenía y los roles que ostenta-

ba en el desarrollo de la aplicación.

Los documentos que dan prueba de ello son:

a) La carta de 9 de junio de 2020 de Directora General de Salud Pública, Calidad e Innovación.

b) El Acuerdo del Consejo Interterritorial de 19 de agosto de 2020.

c) y el Acuerdo (publicado en el BOE el 15 de octubre de 2020) entre el METD y el MSND acerca de la aplicación Radar Covid.

La AEPD hace un prolijo razonamiento para señalar, que a su juicio, la SEDIA ha jugado, con claridad, el rol de responsable del tratamiento, pero en los documentos que se han citado, la SEDIA siempre figura como encargada del tratamiento y sus actuaciones han ido siempre dirigidas a cumplir esta función.

Cabe hacer referencia al valor que la resolución del procedimiento sancionador otorga a las Notas de Prensa del METD, en el sentido de que, si bien considera que no atribuyen competencia alguna sobre la actuación de la SEDIA; son una prueba más de la actividad desarrollada por la SEDIA en la aplicación Radar Covid. Considera la SEDIA que son simples anuncios que realizados por el METD para informar a la ciudadanía y los medios de comunicación, de actividades que estaban proyectadas o en curso de realización. Tienen un valor de difusión y publicidad, en ningún caso pueden ser consideradas, como un elemento del que se pueda inferir, tal como señala la AEPD, que estas Notas de Prensa publicadas por el METD, pongan de manifiesto que la SEDIA, desde un principio actuó como responsable del tratamiento. No pueden servir para adjudicar roles de responsable del tratamiento ni de encargado del tratamiento, ya que son meros documentos informativos y no atributivos de competencias.

Tampoco cabe adjudicar a la SEDIA, como se indica en la resolución del procedimiento sancionador, el rol de responsable de tratamiento solo porque, a través de la SGAD, fuera el órgano encargado de celebrar el "Acuerdo de contratación" que tuvo por objeto la contratación de los servicios de diseño desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación con la pandemia ocasionada por la COVID-1, ya que, también ha sido la encargada de realizar el contrato necesario para el desarrollo de la app, con el rol de encargada de tratamiento en sucesivas fases.

La SEDIA, a través de la SGAD ha desarrollado estas y otras aplicaciones, y ha desarrollado una labor de difusión que probablemente el MSND no estaba en condiciones de hacer porque la situación de pandemia exigía una mayor dedicación a otros asuntos más relevantes en el ámbito de sus competencias.

De cara a la ciudadanía, y tal y como se ha señalado, fue el Gobierno el que impulsó la creación de esta aplicación e instó a la población al uso de Radar Covid, por lo que, no cabe afirmar que fuera la SEDIA la que, por los anuncios de prensa, tuviera una apariencia para la ciudadanía como responsable del tratamiento cuando su papel era simplemente contribuir, en colaboración con todo el Gobierno a aportar soluciones en el ámbito de sus competencias de impulso

de la digitalización de las administraciones públicas (y todo ello sin tener en cuenta que la propia existencia de categorías jurídicas como las de responsable y encargado del tratamiento de protección de datos son difícilmente aprehensibles para el común de los destinatarios de una nota informativa ministerial, ni siquiera para operadores jurídicos no especializados, y pretender que la población general pueda extraer las conclusiones y la subsiguiente atribución de roles que plantea la propuesta de resolución de la lectura de una nota de prensa y traer anudados unos incumplimientos de la normativa vigente excede, a nuestro juicio, lo razonable).

El hecho de colaborar, impulsar y tener un papel relevante en intentar convencer a la población del uso de Radar Covid, para prevenir los contagios y reducir los ingresos hospitalarios y con ello las muertes, ofreciendo una explicación de las características de la aplicación en los medios de comunicación, no puede llevar a la conclusión de que se esté desarrollando otro papel diferente al asignado en los documentos reiteradamente señalados.

Sólo puede entenderse esta participación desde el punto de vista de una actuación coordinada del Gobierno en el que todos los departamentos contribuían, en un Estado de alarma declarado a limitar las consecuencias de la pandemia. Conviene recordar, que no fue hasta el 6 de agosto de 2020, cuando se publicó la modificación de la estructura del MSND con la creación de la Secretaría General de Salud Digital y la Dirección General de Digitalización, con la consiguiente atribución de nuevas competencias en materia de digitalización de la salud y de elaboración de Apps en materia sanitaria a este departamento.

IV

La SEDIA, en su condición de encargado de tratamiento, contó desde el primer momento, con la autorización del MSND, como responsable del tratamiento, para la contratación de INDRA, que, contaba con las garantías suficientes para garantizar la aplicación del RGPD. Las reuniones en las que el MSND daba instrucciones al encargado de tratamiento, la SEDIA, sobre la prueba piloto, se celebraban con la presencia de representantes de esta empresa.

V

El derecho a la protección de datos, como cualquier otro derecho, no es absoluto. La aplicación de su normativa debe ser modulada y tener en cuenta la realidad social del tiempo en el que se aplica (como fue el caso de la situación excepcional constituida por la emergencia sanitaria y el estado de alarma), y la posible colisión o concurrencia con otros derechos.

No basta con atenerse a la aplicación literal de una norma, sin apelar, ni tener en cuenta su espíritu y finalidad tal como prescribe el artículo 3 del Código Civil. La exigencia y aplicación de la normativa de protección de datos, en unas circunstancias tan especiales y atípicas, y sin perjuicio del respeto al principio de seguridad jurídica, debe ser equilibrada y ponderada.

En ningún momento los organismos responsables de la protección de datos

pueden actuar como si el estado de alarma no hubiese existido o no afectase a la materia de su competencia y al ejercicio de sus facultades.

En la fase de aplicación del piloto, hay que considerar que los datos recopilados y generados por la aplicación no permiten, por defecto, la identificación directa del usuario o de su dispositivo. Sin embargo, aunque, ateniéndonos al considerando 30 del RGPD, los usuarios podrían llegar a ser identificables mediante la asociación de algún identificador en línea facilitado por el dispositivo u otro tipo de herramientas o protocolos, en el proyecto piloto los datos no eran reales (eran de prueba) y los códigos de contagiados para su introducción en la App eran falsos. Cuando la App se abrió en La Gomera al público, las personas no podían introducir datos reales de estar infectados.

El tratamiento de estos datos por Radar Covid ha sido lícito, cabe recordar a este respecto con el Informe AEPD 17/2020, de 12 de marzo, que el RGPD prevé que la base jurídica que otorga licitud a este tipo de tratamiento (más allá de los casos en donde preste consentimiento el interesado), la encontramos en los artículos 6.1.d) (cuando sea necesario para proteger intereses vitales del interesado u otras personas físicas) y 6.1.e) (cuando sea necesario para el cumplimiento de una misión realizada en interés público).

VI

Si bien la EIPD publicada en septiembre 2020 fue la versión 1.1, ya existía una versión 1.0 del EIPD, mucho más preliminar y básica, con anterioridad al 19 de agosto de 2020. La EIPD facilitada a la AEPD fue la versión 1.1 pues es la que se publicó, coincidiendo con el despliegue en septiembre 2020 de una versión de la aplicación, con soporte de lenguas cooficiales. Durante el periodo que va del 19 de agosto hasta la publicación en septiembre 2020, se debatió internamente sobre la conveniencia o no de la publicación de dicho documento.

Señala la AEPD, en su resolución del procedimiento sancionador que la realización posterior de la EIPD no "subsana" la falta de realización de esta en el momento oportuno y con la participación de todos los actores necesarios, especialmente porque la falta de evaluación de los riesgos y de adopción de las medidas técnicas y organizativas oportunas, ya ha producido un daño intangible en los derechos y libertades de los ciudadanos, más reprochable si se trata de Administraciones Públicas. Conviene recordar en este punto que la aplicación piloto de RADAR COVID utilizaba datos simulados por lo que si bien, la EIPD se hizo en un momento posterior a la puesta en funcionamiento del piloto, sí se hizo con anterioridad al momento en que la aplicación iba a manejar datos de salud reales de los usuarios.

VII

Respecto a las afirmaciones de la AEPD en la resolución del procedimiento sancionador relativas a las condiciones de uso y la política de privacidad, el equipo de Radar Covid, ha ido revisando y actualizando los documentos con el ánimo de mejorar su contenido y facilitar su lectura y comprensión, haciendo uso de su facultad de responsabilidad proactiva en la mejora constante de la

app y su documentación asociada.

Por otra parte, cualquier cambio de la aplicación incluyendo nuevas funcionalidades (como la conexión de RADAR COVID al nodo europeo de interoperabilidad) ha conllevado la actualización de las condiciones de uso y política de privacidad, a fin de aportar transparencia e información a las personas usuarias de la aplicación.

Las condiciones de uso y política de privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es. Por ende, es necesario el consentimiento expreso del usuario para poder utilizar la aplicación, además de ser su uso totalmente voluntario.

Por otra parte, conviene resaltar que en el tiempo que la aplicación lleva operativa, la SEDIA no ha recibido ninguna queja, ni formal ni informal, del Delegado de Protección de Datos del Ministerio de Sanidad en relación a la aplicación Radar Covid.

VIII

Respecto a las vulnerabilidades detectadas el equipo de desarrollo no consideró necesario resolver este problema en las primeras versiones dado que, para explotar esta vulnerabilidad se debía presuponer un remoto escenario donde el operador de telecomunicaciones estuviera interesado en obtener esta información clínica de sus clientes estudiando el tráfico de datos generado por la App Radar Covid.

La vulnerabilidad fue analizada y se programó una corrección coincidiendo con una próxima liberación de la aplicación. Fue corregida el 8 de octubre de 2020, y compartido el código que corregía el problema con el equipo técnico de la Escuela Politécnica Federal de Lausana (EPFL), que es quien había impulsado el protocolo DP3-T, garante de la privacidad.

La corrección fue atendida en plazos razonables de tiempo de acuerdo con su impacto.

Ese juicio se mostró acertado, pues no se ha detectado ni se tiene constancia de que esta teórica vulnerabilidad haya sido explotada o aprovechada en ningún caso real, seguramente por la dificultad y poco beneficio que se obtendría de su implantación.

Es conocido por todos que no existe ningún sistema informático 100% seguro, y por ello se optó, una vez ponderadas estas circunstancias por continuar el desarrollo (aplicando el principio "in dubio pro actione"). Dado que la alternativa era paralizar el uso y desarrollo de la app con el consiguiente riesgo y menoscabo para la salud colectiva, al privar a la sociedad de una herramienta con un gran potencial de ayuda en pleno estado de alarma por emergencia sanitaria.

IX

Como conclusión cabe afirmar que puede haber discrepancias en los criterios sobre las actuaciones en las que se ha concretado el trabajo de puesta en marcha, en un tiempo razonable, de una aplicación necesaria en el contexto de pandemia en el que se desarrolló, con un estado de emergencia declarado. Pero siempre ha actuado con una responsabilidad proactiva para corregir los posibles errores u omisiones de la App, asumiendo el principio de privacidad desde el diseño, actuando en defensa del interés público y de la ciudadanía, y colaborando con la AEPD en todo lo solicitado. Como ya señalamos anteriormente y ahora repetimos, la situación de emergencia y la declaración el estado de alarma alteró el Orden Jurídico ordinario y el modo de actuar habitual de la Administración. La situación excepcional determinó una modulación en los procedimientos de la administración y exigió actuar con celeridad para así poder llegar a tiempo y que la aplicación cumpliera con sus fines en un momento en que todos los gobiernos de nuestro entorno europeo e internacional, la estaban demandando. Y hubo que desarrollar una aplicación piloto con datos simulados, hubo que hacer la contratación de emergencia en que se suprimieron trámites esenciales, en favor de la agilidad, y hubo que extender rápido la aplicación a las CCAA a través de los instrumentos jurídicos más inmediatos y acordes con la situación que permitieran cohonestar la cobertura jurídica y la agilización de trámites burocráticos.

Se hicieron las evaluaciones pertinentes, los análisis que permitió la premura con que hubo de desarrollarse la aplicación y se actuó siempre con la finalidad última de ejercer una responsabilidad proactiva para permitir un adecuado respeto a la protección de datos de carácter personal. En definitiva, conforme a las argumentaciones y razonamientos anteriores, la SEDIA considera que no ha lugar a sanción de apercibimiento, porque no ha existido un incumplimiento flagrante, consciente y deliberado de la normativa de protección de datos y de todos los artículos que se citan en la resolución del procedimiento sancionador.

Por último, solicita que se deje sin efecto la resolución recurrida y mediante otrosí, argumenta que, como quiera que se denegó a la SEDIA la práctica de la prueba solicitada con fecha 10 de febrero de 2022, que figura en el epígrafe IV CONSIDERACIONES COMPLEMENTARIAS de los Fundamentos de Derecho de la resolución del procedimiento sancionador, solicita que en el plazo más breve posible se le haga llegar la documentación solicitada.

FUNDAMENTOS DE DERECHO

I

Es competente para resolver el presente recurso la Directora de la Agencia Española de Protección de Datos, de conformidad con lo dispuesto en el artículo 48.1 de la LOPDGDD y el artículo 123 de la LPACAP.

II

Debido a razones de funcionamiento del órgano administrativo, por ende no atribuibles a la SEDIA, hasta el día de la fecha no se ha emitido el preceptivo pronunciamiento de

esta Agencia respecto a la pretensión del interesado.

De acuerdo con lo establecido en el artículo 24 de la LPACAP el sentido del silencio administrativo en los procedimientos de impugnación de actos y disposiciones es desestimatorio.

Con todo, y a pesar del tiempo transcurrido, la Administración está obligada a dictar resolución expresa y a notificarla en todos los procedimientos cualquiera que sea su forma de iniciación, según dispone el artículo 21.1 de la citada LPACAP. Por tanto, procede emitir la resolución que finalice el procedimiento del recurso de reposición interpuesto.

III

En relación con las manifestaciones efectuadas por la SEDIA, que reiteran básicamente las alegaciones ya presentadas a lo largo del procedimiento sancionador, debe señalarse que todas ellas ya fueron analizadas y desestimadas en los Fundamentos de Derecho (en adelante, FD) de la Resolución recurrida, tal como se transcribe a continuación:

En el FD IV, se decía:

"(…)

A) Respecto de las ALEGACIONES DE CARÁCTER GENERAL:

Alude a RADAR COVID como una herramienta adicional y al Real Decreto 463/2020, de 14 de marzo. Aduce que, en ese contexto, la SEDIA, como encargada de tratamiento, actuó conforme a las indicaciones dadas en todo momento por el MSND, como autoridad delegada del Gobierno en materia de salud pública y responsable del tratamiento. Razona que, aunque estas indicaciones no se plasmaron conforme exige la normativa, se debió a que el estado de alarma dificultó la formalización de los instrumentos habituales previstos en la legislación para estos supuestos en circunstancias normales. Alude a las reuniones celebradas a las que asistieron representantes del MSND, de la SEDIA y de la empresa adjudicataria del contrato de emergencia, en las que se tomaban las decisiones necesarias para avanzar en el desarrollo del piloto y de la aplicación.

En este sentido, de la práctica de la prueba y en relación con las reuniones celebradas y que constan en los hechos probados, no se ha acreditado la existencia de ninguna indicación "instrucción" por parte del MSND que dé cobertura a las actuaciones desarrolladas por la SEDIA. Tampoco en la carta referenciada de 9 de junio de 2020, dando el visto bueno para el desarrollo de la aplicación móvil. Y respecto de toda la comunicación y contactos que dice haber mantenido con el MSND tampoco aporta prueba alguna, ni tan siquiera un correo electrónico.

En todo caso, estas "indicaciones" a las que alude, no son suficientes para articular la relación entre responsable y encargado del tratamiento, relación que no puede ser considerada como una mera formalidad administrativa o como un intercambio de opiniones, sino como un medio para procurar la defensa y la protección del De-

recho Fundamental a la protección de datos de carácter personal, máxime cuando la relación se establece entre los órganos de una misma Administración Pública o entre distintas Administraciones Públicas a quienes corresponde "promover las condiciones para que la libertad y la igualdad del individuo y de los grupos en que se integra sean reales y efectivas; remover los obstáculos que impidan o dificulten su plenitud y facilitar la participación de todos los ciudadanos en la vida política, económica, cultural y social", artículo 9.2 de la Constitución Española.

En conclusión, no se ha acreditado la existencia de las instrucciones recibidas del responsable del tratamiento, en los términos anteriormente descritos, desconociéndose su contenido, ámbito, asuntos, fechas en las que fueron suministradas, ni cuál ha sido la actuación, respuesta y reporte suministrado por la SEDIA, consecuencia de estas.

En todo caso, aún cuando hubieran acreditado comunicaciones informales entre las partes para suministrar instrucciones, hemos de significar que el artículo 28.1.a) del RGPD impone que las instrucciones que rigen la relación entre responsables y encargados del tratamiento se encuentren documentadas. Y es que, las instrucciones a las que hace mención el RGPD no dejan de ser documentos internos con efectos en la relación entre el responsable y el encargado del tratamiento en el marco de un contrato de encargado del tratamiento; contrato de encargado de tratamiento u otro acto jurídico que no existe en el presente supuesto.

Por consiguiente, no queda acreditado por parte de la SEDIA que actuase siguiendo las instrucciones del MSND.

B) Respecto de las ALEGACIONES ESPECÍFICAS:

B.1 Respecto al tratamiento de datos de carácter personal.

Alude a que, el derecho a la protección de datos no es absoluto e invoca el artículo 3 del Código Civil. Aduce que, la exigencia y aplicación de la normativa de protección de datos en unas circunstancias tan especiales y atípicas, debe ser equilibrada y ponderada y que, la Agencia no puede actuar como si el estado de alarma no hubiese existido.

En este sentido, el derecho fundamental a la protección de datos no se suspende por la mera declaración de un estado de alarma, sino que esta suspensión queda limitada a los supuestos de declaración del estado de excepción o de sitio, según establece el artículo 55.1 de la CE. En el estado de alarma sólo puede condicionarse el ejercicio de los derechos, pero no suspenderlos.

En este supuesto concreto, se declaró el estado de alarma, lo que no supuso, en ningún caso la suspensión de los derechos fundamentales.

Además, la propia normativa de protección de datos personales (RGPD) contiene las salvaguardas y reglas necesarias para permitir legítimamente los tratamientos de datos personales en situaciones, como la que aconteció, en que existía una emergencia sanitaria de alcance general.

También aduce que los datos no eran reales (eran de prueba), que los códigos de contagiados para su introducción en la App eran falsos y que cuando la App se abrió en La Gomera al público, las personas no podían introducir datos reales de estar infectados. En concreto, esta alegación será objeto de análisis en el FD V de esta Resolución.

Invoca la licitud del tratamiento y se remite al Informe de la AEPD 17/2020, de 12 de marzo, destacando la base relativa a los artículos 6.1.d) y 6.1.e) del RGPD. Efectivamente, el tratamiento de los datos debe basarse en una causa lícita (artículo 6 RGPD) y debe ser transparente para los afectados (artículos 13 y 14 del RGPD). Por tanto, la falta de información o transparencia supone un incumplimiento de los principios de protección de datos. Este aspecto será analizado en el FD IX de esta Resolución.

B.2 Respecto al rol de la SGAD en el tratamiento de datos

1º. La etapa en la que se hace el proyecto piloto.

Alude de nuevo al visto bueno recibido en fecha 9 de junio de 2020 por parte de la Dirección General de Salud Pública (sic) del MSND donde se considera como responsable del tratamiento de los datos del piloto a la autoridad sanitaria de la Comunidad en que se fuera a llevar a cabo. Analizaremos estos hechos en el FD VII de esta Resolución.

Respecto a la siguiente afirmación realizada por la SEDIA: "Quedando la SEDIA como encargada del tratamiento de los datos y resultados", nada se dice al respecto en el mandato recibido en fecha 9 de junio de 2020.

Coincide esta Agencia en que ha quedado acreditada la participación de la DGSP, antes DIRECCIÓN GENERAL DE SALUD PÚBLICA, CALIDAD E INNOVACION, en las reuniones semanales del piloto para la conformación de los fines y medios del proyecto. De igual modo, la misma afirmación puede realizarse respecto a la participación de la SEDIA.

Y, aunque los datos relativos a la salud manejados en el piloto fueran datos simulados de infección (datos no reales), se trataron datos personales, cuestión que será desarrollada en el FD V de esta Resolución.

2º.- La etapa en la que se pone en marcha la aplicación en fase de pruebas y posteriormente la aplicación definitiva.

Alude al Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, de 19 de agosto de 2020, que permitió que las CCAA pudieran asumir temporalmente, hasta la firma de los convenios, la gestión de los códigos de diagnóstico positivo y a la hoja de ruta presentada por el Presidente del Gobierno para hacer frente al ascenso de la "segunda curva epidemiológica", que entre otras medidas citó, el refuerzo de los medios digitales de rastreo, solicitando a los ciudadanos el uso de RADAR COVID. Aduce que, en el Acuerdo, de 9 de octubre de 2020, que faculta a la SGAD para la suscripción de Convenios con Comunidades y Ciudades Autónomas, se especifica lo siguiente: "en los mencionados Convenios de colaboración, el

Ministerio de Sanidad y la Consejería competente en materia de sanidad de la Comunidad o Ciudad Autónoma de que se trate figurarán como responsables del tratamiento de datos de carácter personal y ***la SGAD como encargado del tratamiento.****" Y especifica parte de las atribuciones que según su condición, competen a unos y a otros.*

Nada nuevo aporta esta alegación que ya fue objeto de un pormenorizado análisis en la propuesta de resolución (FD VII) y que de nuevo será rebatida en el FD VII de esta Resolución.

No coincide la AEPD con la afirmación realizada por la SEDIA respecto a que haya quedado plenamente acreditado que en todo momento y de acuerdo con los instrumentos jurídicamente vinculantes, la SGAD actuase única y exclusivamente como encargada del tratamiento, pues no es hasta que se celebra el acuerdo de Acuerdo del Consejo Interterritorial del Sistema Nacional de Salud, de 19 de agosto de 2020, cuando, por primera vez, se le reconoce esta condición.

Por añadidura, según el hecho probado vigésimo séptimo, la primera versión de la EIPD, de 12 de agosto de 2020, en cuanto a los roles de "Responsables, corresponsables y encargados del tratamiento" disponía:

En este caso el ***titular de la aplicación es la Secretaría General de Administración Digital*** *dependiente del Ministerio de Asuntos Económicos y Transformación Digital,* ***que también se constituye como Responsable del Tratamiento****.*

La aplicación ha sido desarrollada a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA).

Por otra parte, la SEDIA ha facilitado dos enlaces que dirigen a dos documentos del MSND:

1. Estrategia de detección precoz, vigilancia y control de covid-19.

2. Procedimiento de implementación de la app Radar COVID como complemento a los sistemas manuales de identificación de contactos, coordinado por el Centro de Coordinación de Alertas y Emergencias Sanitarias, Dirección General de Salud Pública, Calidad e Innovación y aprobado por la Ponencia de Alertas y Planes de Preparación y Respuesta.

E insiste en que, en todo momento, tanto en el desarrollo del piloto, como en el uso de RADAR COVID en pruebas por las CCAA, y en su uso, superada dicha fase de pruebas, estaban definidos los roles de responsable y encargado de tratamiento, y remite de nuevo, a la carta de 9 de junio de 2020, al Acuerdo del Consejo Interterritorial y al Acuerdo publicado en el BOE el 15 de octubre.

En relación con este argumento, nos remitimos a lo anteriormente expuesto. La SEDIA no aparece como encargada del tratamiento hasta que se produce el Acuerdo del Consejo Interterritorial. El RGPD enumera los elementos que deben establecerse en el contrato o acto jurídico (artículo 28.3 RGPD). No obstante, el acuerdo del Consejo Interterritorial únicamente disponía: El encargado del tratamiento será, en ambos casos, la Secretaría de Estado de Digitalización e Inteligencia Artificial. Es

decir, no estipuló, ninguna otra información más específica y concreta sobre cómo se cumplirían los requisitos del acuerdo. Con posterioridad, a partir del Acuerdo publicado en el BOE el 15 de octubre, la que aparecerá como encargada del tratamiento será la SGAD.

En definitiva, la SEDIA, aparece como encargada del tratamiento a partir del Acuerdo del Consejo Interterritorial y ejerce esta condición hasta que se produce la celebración de los correspondientes convenios con las CCAA, en los que asumirá la condición de encargada del tratamiento, la SGAD.

En cuanto a la disconformidad de la SEDIA con alguna de las afirmaciones realizadas por la Agencia respecto a las Notas de Prensa del METD, por cuanto no atribuyen competencia alguna, esta cuestión no es discutida por la Agencia.

El artículo 2.1 de la Ley 50/1997, de 27 de noviembre, del Gobierno dispone: El Presidente dirige la acción del Gobierno y coordina las funciones de los demás miembros del mismo, sin perjuicio de la competencia y responsabilidad directa de los Ministros en su gestión.

Asimismo, el artículo 3.1.d) de la Ley 3/2015, de 30 de marzo, reguladora del ejercicio del alto cargo de la Administración General del Estado, aplicable a los miembros del Gobierno y los Secretarios de Estado, dispone la observancia del principio de transparencia y responsabilidad en los siguientes términos: adoptarán sus decisiones de forma transparente y serán responsables de las consecuencias derivadas de su adopción.

Por otra parte, la LRJSP, en el artículo 3.1.c) dispone que las Administraciones Públicas deben respetar en su actuación y relaciones una serie de principios, entre ellos, la transparencia de la actuación administrativa.

Asimismo, la Ley 19/2013, de 9 de diciembre, de transparencia, acceso a la información pública y buen gobierno, en el artículo 26 bajo el epígrafe "Principios de buen gobierno", dispone que las personas comprendidas en su ámbito de aplicación (miembros del gobierno, Secretarios de Estado, resto de altos cargos de la AGE, etc.) adecuarán su actividad a los "Principios de actuación", entre ellos, el previsto en el apartado 7º que se refiere al desempeño de sus funciones con transparencia.

En suma, las notas de prensa, más allá de ser consideradas según afirma la SEDIA, como "simples anuncios que realizó el METD para informar a la ciudadanía y los medios de comunicación, de actividades que estaban proyectadas o en curso de realización", difundieron información por parte del METD, facilitando el conocimiento por la ciudadanía de la información relativa al rastreo de contactos y las decisiones adoptadas al respecto.

Son por tanto, una prueba más, de la actividad desarrollada por la SEDIA en relación con la aplicación Radar COVID.

En cuanto a que fue el Gobierno el que impulsó la creación de esta aplicación e instó a la población al uso de RADAR COVID, hay que señalar que, el artículo 97 de la

Constitución atribuye al Gobierno funciones políticas y ejecutivas, un binomio que tiene su reflejo en toda acción de gobierno y que se proyecta, también, sobre la relación comunicativa que en un sistema democrático existe entre gobernantes y gobernados.

El Gobierno es, indudablemente, sujeto y objeto de información y valoración política; pero, en cuanto responsable último de la Administración General del Estado (en lo sucesivo, AGE) y en razón, precisamente, de la función ejecutiva que constitucionalmente se le encomienda, es emisor de una serie de mensajes dirigidos a los ciudadanos que se engloban bajo la denominación genérica de campañas institucionales de publicidad y de comunicación, según se recoge en la exposición de motivos de la Ley 29/2005, de 29 de diciembre, de Publicidad y Comunicación Institucional.

La SEDIA rechaza la interpretación de la Agencia sobre su papel de cara a la ciudadanía, y alega que, simplemente contribuyó, en colaboración con todo el Gobierno, a aportar soluciones en el ámbito de sus competencias de impulso de la digitalización de las administraciones públicas (y todo ello, sin tener en cuenta la existencia de categorías jurídicas como las de responsable y encargado del tratamiento de protección de datos difícilmente aprehensibles para el común de los destinatarios).

Pues bien, las categorías jurídicas a las que se refiere son conceptos jurídicos determinados en el artículo 4.7) y 4.8) del RGPD y desempeñan un papel crucial en la aplicación del RGPD, puesto que determinan quién responde del cumplimiento de las distintas normas relativas a la protección de datos y cómo pueden los interesados ejercer sus derechos en la práctica.

Respecto a que, por el hecho de colaborar, impulsar y tener un papel relevante en intentar convencer a la población del uso de RADAR COVID y ofrecer explicaciones de las características de la aplicación en los medios de comunicación, no puede llevar a la conclusión de que se esté desarrollando otro papel diferente al asignado en los documentos reiteradamente señalados, nos remitimos a lo dispuesto en las Directrices 07/2020 sobre los conceptos de «responsable del tratamiento» y «encargado del tratamiento» en el RGPD, que en el apartado 25 dice:

"En ausencia de responsabilidad por el tratamiento derivada de disposiciones legales, la calificación de una parte como «responsable del tratamiento» debe establecerse sobre la base de una evaluación de las circunstancias de hecho en que tiene lugar el tratamiento. Para alcanzar una conclusión acerca de si un ente concreto ejerce una influencia determinante en relación con el tratamiento de los datos personales en cuestión, deben tenerse en cuenta todas las circunstancias de hecho pertinentes."

Y las circunstancias de hecho nos remiten al mismo punto de partida. Es decir, al tratamiento de datos personales por parte de la SEDIA durante la ejecución del proyecto piloto, sin contar con un contrato u otro acto jurídico que la vinculase con la Dirección General de Salud Pública, Calidad e Innovación, conforme exige la normativa vigente.

En este sentido, el apartado 102 de las Directrices 07/2020, dice:

"Además, el contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros debe vincular al encargado frente al responsable; esto es, debe imponer al encargado obligaciones vinculantes en virtud del Derecho de la Unión o de los Estados miembros. También debe establecer las obligaciones del encargado. En la mayor parte de los casos, existirá un contrato, pero el Reglamento también hace referencia a «otro acto jurídico», como una norma nacional (de Derecho primario o derivado) u otro instrumento jurídico. Si el acto jurídico no incluye todo el contenido mínimo requerido, debe complementarse con un contrato u otro acto jurídico que incluya los elementos que falten."

B.3 Respecto al rol de INDRA

Alude a que la SEDIA, en su condición de encargado del tratamiento, contó desde el primer momento, con la autorización del MSND, como responsable del tratamiento, para la contratación de INDRA, que, contaba con las garantías suficientes para garantizar la aplicación del RGPD.

Respecto a esta alegación, cabe señalar que en la propuesta de resolución no se imputa la infracción del artículo 28.1 del RGPD.

B.4 Respecto a las Evaluaciones de Impacto

Insiste en que, si bien la EIPD publicada en septiembre 2020 fue la versión 1.1, ya existía una versión 1.0 con anterioridad al 19 de agosto de 2020. La EIPD facilitada a la AEPD fue la versión 1.1 pues es la que se publicó, coincidiendo con el despliegue en septiembre 2020 de una versión de la aplicación, con soporte de lenguas cooficiales.

Aduce que, durante el periodo que va del 19 de agosto hasta la publicación en septiembre 2020, se debatió internamente sobre la conveniencia o no de su publicación. Invoca la personalidad jurídica única de la AGE; añade que, ostenta la condición de responsable y de encargado del tratamiento a través de órganos distintos y no viene publicando ni la EIPD, ni los Análisis de Riesgos sobre las que se basan, de los sistemas que desarrolla.

Razona que la SGAD recabó criterio al delegado de protección de datos del METD. Su criterio fue que, con carácter general, no debían publicarse estos documentos.

En todo caso, finalmente publicó la EIPD y el Análisis de Riesgos en septiembre de 2020.

Por otra parte, cuestiona el criterio de la AEPD, página 189 de la propuesta de resolución, que califica de "más reprochable" la falta de realización de la EIPD en el momento oportuno e insiste en que en ese momento, durante el proyecto piloto, se utilizaron datos simulados, y aunque se hizo en un momento posterior a la puesta en funcionamiento del piloto, se hizo con anterioridad al momento en que la aplicación iba a manejar datos de salud de los usuarios.

En este sentido, la EIPD es una herramienta de carácter preventivo que debe reali-

zar el responsable del tratamiento para poder identificar, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas.

De hecho, otra de las circunstancias que identifican a la SEDIA como responsable del tratamiento, es que, a través de la SGAD, fue el órgano del METD, encargado de celebrar el "Acuerdo de contratación" que tuvo por objeto la contratación de los servicios de diseño, desarrollo, piloto y evaluación de un sistema que permita la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-1, aspecto que desarrollamos en el FD VIII. Confirma este hecho, el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, que exige/encarga una serie de entregables, entre ellos, la EIPD.

B.5 Respecto a las condiciones de uso y política de privacidad

Alude a que, la primera versión de la App (piloto) sirvió a efectos de comprobar aspectos como la usabilidad, percepción de privacidad, y eficacia de la solución en un entorno simulado.

También incluía un aviso sobre la participación voluntaria en una experiencia piloto con datos ficticios de alerta de contagios de la COVID-19 en la isla de La Gomera.

Añade que los documentos se han ido revisando y actualizando con el ánimo de mejorar su contenido y facilitar su lectura y comprensión, haciendo uso de su facultad de responsabilidad proactiva.

Y que con cada actualización del aplicativo se solicitaba de nuevo el consentimiento expreso de los usuarios.

Respecto a los responsables del tratamiento se remite a la Política de Privacidad actual (https://radarcovid.gob.es/politica-de-privacidad) que establece como responsables del tratamiento al MSND y CCAA, y como encargado del tratamiento a la SGAD.

Justifica el incremento de las 700 palabras con las explicaciones más extensas, así como la ampliación a nuevos usos de la aplicación, o la interoperabilidad con las aplicaciones de rastreo de contactos de la Unión Europea, que ha conllevado su actualización, con el fin de aportar transparencia e información a los usuarios.

Recuerda que, las Condiciones de Uso y Política de Privacidad han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es.

Añade que no ha recibido ninguna queja del delegado de protección de datos del MSND y que en el apartado de Preguntas frecuentes del sitio web: https://radarcovid.gob.es/faq-datos-personales-y-privacidad, se recoge determinada información.

Pues bien, es cierto que recoge la información que aduce, que además, se visibiliza con 16 viñetas, cuando en realidad son 9 los aspectos que informa. El RGPD deta-

lla la información que debe facilitarse al interesado en la fase inicial del tratamiento, en el artículo 13, que contemplan las categorías de la información que ha de suministrarse a los interesados cuando los datos se obtengan de este. Esta información tiene el carácter de básica (artículo 11.1 LOPDGDD) y debe facilitarse en forma concisa, transparente, inteligible y de fácil acceso.

De los hechos probados, se extrae la conclusión de que, la transparencia de la información facilitada a lo largo de las distintas fases de implementación del proyecto piloto y de la aplicación Radar COVID, ha sido confusa, prolija y contradictoria, observada desde las distintas fuentes que emanaba.

De hecho, en febrero de 2022, todavía siguen sin informarse los datos de contacto del delegado de protección de datos (en lo sucesivo, DPD).

Una de las claves para poder garantizar la privacidad es poder demostrarla, verificando que el tratamiento es acorde a la información facilitada. La transparencia de datos se asienta como pilar para demostrar la diligencia y la responsabilidad proactiva ante la autoridad de control y como medida de confianza ante los sujetos cuyos datos son tratados. Tal y como establece el considerando 39 del RGPD, para la personas físicas debe quedar totalmente claro que se están recogiendo, utilizando, consultando o tratando de otra manera datos personales que les conciernen, así como la medida en que dichos datos son o serán tratados.

Por último, otras de las circunstancias de hecho que identifican a la SEDIA como responsable del tratamiento, es que, se identificó a la SGAD como titular de la aplicación, y fue esta la que definió el contenido de las Condiciones de Uso y la Política de Privacidad de la aplicación. Recordemos que es el responsable del tratamiento el que debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto (considerando 78 RGPD).

B.6 Respecto a las vulnerabilidades detectadas

Razona que se juzgó muy remoto el escenario en el que podía explotarse la vulnerabilidad, con un tercero con capacidad suficiente de espiar las redes de comunicaciones y de cruzar la información remitida por RADAR COVID, que permitieran establecer una relación entre la identidad del usuario y su condición médica de positivo por COVID-19.

Aduce que ese juicio se mostró acertado, pues no se ha detectado ni se tiene constancia de que esta teórica vulnerabilidad haya sido explotada o aprovechada y que no existe ningún sistema informático 100% seguro, y por ello, se optó, una vez ponderadas estas circunstancias, por continuar el desarrollo.

El hecho de que la vulnerabilidad fuera corregida no supone que la infracción no se cometiera.

Cualquier aplicación que vaya a utilizar datos personales debe ser concebida y diseñada desde cero identificando, a priori, los posibles riesgos a los derechos y libertades de los interesados y minimizarlos para que no lleguen a concretarse en daños.

Cabe traer a colación, de nuevo, a los "Antecedentes" del "Pliego de condiciones

para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, que decía lo siguiente:

"Siendo de interés general para el Gobierno de la Nación dar respuesta al objetivo común de contribuir a la gestión de la situación de crisis sanitaria ocasionada por el COVID-19, la ***Secretaría de Estado de Digitalización e Inteligencia Artificial*** *del Ministerio de Asuntos Económicos y Transformación Digital, a través de la Secretaría General de Administración Digital (SGAD en adelante),* ***desarrollará un conjunto de actividades para la definición y construcción de un sistema*** *que permita el rastreo de contactos estrechos (de forma segura y anónima para el usuario) y su posterior evaluación a través de un piloto.*

En relación a las tecnologías habilitadoras para el rastreo de contactos, hay que reseñar que Apple y Google, empresas que manejan los sistemas operativos instalados en la práctica totalidad de dispositivos móviles a nivel mundial, anunciaron el pasado 10 de abril de 2020 una alianza para crear un sistema interoperable, integrado en los sistemas operativos iOS y Android, para el seguimiento de contactos, que no utiliza geolocalización sino Bluetooth de baja energía (Bluetooth LE o BLE), para identificar dispositivos presentes a una distancia próxima.

El enfoque de Apple/Google está basado en el protocolo DP-3T, que preserva la privacidad mediante el empleo de identificadores efímeros sobre los que no es posible realizar ingeniería inversa para obtener datos personales del propietario del dispositivo. Apple y Google liberaron el kit para desarrolladores (SDK, https:// apple.com/covid19/contracttracing) el pasado 20 de mayo, lo que permite a los distintos Estados desarrollar soluciones de rastreo de contactos sobre las nuevas funciones incorporadas en sus sistemas operativos, siempre bajo la tutela de las autoridades sanitarias nacionales.

El Sistema que se desarrollará mediante este contrato hará uso de este SDK, *sobre el que se construirá una aplicación móvil que permita activar el sistema de rastreo de contactos; que en conexión con las autoridades sanitarias pueda recibir un código de confirmación de positivo en COVID-19; y que mediante una plataforma servidora (backend) con la que se comunica la aplicación móvil se pueda alertar a las personas con las que se ha tenido un contacto estrecho en fechas recientes.*

Este hecho apunta una vez más, a que la SEDIA, determinó parte de los medios esenciales del tratamiento al decidir utilizar tecnología Bluetooth siguiendo el modelo descentralizado basado en el protocolo DP-3T.

En este sentido, las Directrices 07/2020 en su apartado 40 indican:

Por lo que respecta a la determinación de los medios, cabe distinguir entre los medios esenciales y los no esenciales. ***Los medios esenciales se reservan tradicionalmente y de forma inherente al responsable del tratamiento.*** *Estos deben ser determinados obligatoriamente por el responsable del tratamiento aunque la determinación de los medios no esenciales también puede dejarse en manos de él. Los medios esenciales son medios estrechamente ligados al fin y el alcance del tratamiento, como el tipo de datos personales tratados («¿qué datos se tratarán?»), la*

duración del tratamiento («¿cuánto tiempo se tratarán?»), las categorías de destinatarios («¿quién tendrá acceso a los datos?») y las categorías de interesados («¿a quién pertenecen los datos personales tratados?»). Además de estar relacionados con el fin del tratamiento, los medios esenciales se encuentran estrechamente vinculados a la cuestión de si el tratamiento es lícito, necesario y proporcionado.

III. CONCLUSIÓN DEL ESCRITO DE ALEGACIONES

Alude la SEDIA a que es consciente que puede haber discrepancias en los criterios sobre las actuaciones en las que se ha concretado el trabajo de puesta en marcha de una aplicación necesaria en el contexto de pandemia, con un estado de emergencia declarado. Añade que siempre ha actuado con responsabilidad proactiva colaborando con la AEPD en todo lo solicitado.

De hecho, alega que solicitó informe a la AEPD en el momento en que estaba prevista la extensión de la aplicación a las CCAA en agosto de 2020, momento en el que habría sido muy valiosa la aportación de la AEPD, pero el inicio de las actuaciones previas, determinó, a juicio de la AEPD, la imposibilidad de contar con este informe.

Insiste en que la situación de emergencia y la declaración el estado de alarma alteró el orden jurídico ordinario y el modo de actuar habitual de la Administración.

La situación excepcional determinó una modulación en los procedimientos de la administración y exigió actuar con celeridad para así poder llegar a tiempo y que la aplicación cumpliera con sus fines.

Se hicieron las evaluaciones pertinentes, los análisis que permitió la premura con que hubo de desarrollarse la aplicación y se actuó siempre con la finalidad última de ejercer una responsabilidad proactiva para permitir un adecuado respeto a la protección de datos de carácter personal.

En definitiva, conforme a las argumentaciones y razonamientos anteriores, la SEDIA considera que no ha lugar a sanción de apercibimiento, porque no ha existido un incumplimiento flagrante, consciente y deliberado de la normativa de protección de datos y de todos los artículos que se citan en la propuesta de resolución del expediente sancionador.

Respecto a las conclusiones alcanzadas por la SEDIA cabe señalar lo siguiente:

La normativa de protección de datos personales, en tanto que dirigida a salvaguardar un derecho fundamental, se aplicó en su integridad durante el estado de alarma declarado, dado que no produjo la suspensión de derecho fundamental alguno, siendo la postura adoptada por esta Agencia de estrecha colaboración con todas las autoridades públicas que han solicitado su asesoramiento previo durante la pandemia, singularmente con el Ministerio de Sanidad, habiendo ofrecido la AEPD su colaboración en distintas ocasiones a la SEDIA, vía email, en fechas 7 y 8 de mayo de 2020, interesándose por el grupo de trabajo en el que participaba la SEDIA para coordinar con las CCAA el despliegue de la aplicación.

Tanto es así, que con fecha 7 de abril de 2020, la AEPD informó a petición de la Di-

rectora del Gabinete de la SEDIA, sobre el Convenio tipo con las Comunidades Autónomas para el desarrollo de la aplicación "APP" coronavirus. Sobre dicho Convenio también se emitió el informe 030/2020, de fecha 6 de abril de 2020. Todos estos informes se solicitaron con carácter previo al desarrollo de las aplicaciones, sin que existiesen actuaciones previas iniciadas por esta Agencia.

Por otro lado, la SEDIA alega que solicitó informe a la AEPD en el momento en que estaba prevista la extensión de la aplicación a las CCAA en agosto de 2020, momento en el que habría sido muy valiosa la aportación de la AEPD, pero el inicio de las actuaciones previas, determinó, a juicio de la AEPD, la imposibilidad de contar con este informe. Como bien sabe la SEDIA, sí que se le suministraron observaciones al borrador de "Convenio entre la Secretaría de Estado de Digitalización e Inteligencia Artificial y la Consejería de Sanidad de la Comunidad Autónoma de….sobre la adhesión al uso de la aplicación RADAR COVID19", tal y como ella admite en el escrito de 1 de septiembre de 2020 en el que contestan a un requerimiento de información de 18 de agosto de 2020 (notificado el día 29 del mismo mes y año). No obstante, debe matizarse que dichas observaciones realizadas por el Gabinete Jurídico, no se refieren al objeto de este procedimiento sancionador, sino que están relacionadas únicamente con el borrador del convenio precitado.

Finalmente, en cuanto a la alegada situación de emergencia, por razón del principio de legalidad, de acuerdo con el artículo 9 de la Constitución Española, los ciudadanos y los poderes públicos están sujetos a la Constitución y al resto del ordenamiento, sin que existiera, como se ha indicado, una suspensión del derecho fundamental a la protección de datos personales, tal y como tempranamente indicó esta Agencia en su informe 17/2020.

IV. CONSIDERACIONES COMPLEMENTARIAS

En cuanto a la solicitud de la práctica de la prueba consistente en la puesta a disposición de la SGAD de la siguiente documentación que se considera fundamental para el ejercicio de la defensa en el procedimiento sancionador:

a) Propuesta de resolución del Instructor/a en relación con el procedimiento abierto contra el MSND, a fin de apreciar el criterio de la AEPD en relación con la actividad desarrollada por dicho departamento que aunque goza de la misma personalidad jurídica que la SEDIA, es tratada por la AEPD como un ente distinto.

b) Informes íntegros del Gabinete Jurídico de la AEPD citados que se citan en el Fundamento de Derecho Noveno (17/2020 y 32/2020) de la Propuesta de Resolución, para poder apreciarlo en su conjunto y aceptarlo o rebatirlo según sea su criterio.

Debe desestimarse la solicitud de práctica de prueba realizada por la SEDIA en su escrito de alegaciones -también solicitada en oficio a parte-, y ello en la medida que, la SEDIA, no formuló proposición de prueba alguna en el momento procedimental pertinente, a saber, su escrito de alegaciones presentado en fecha 22 de noviembre de 2021.

Es preciso subrayar, que en el curso del procedimiento, la SEDIA ya se benefició de un período extraordinario de prueba por un plazo de diez días adicionales a los

30 inicialmente concedidos. Es decir, la práctica de prueba abarcó el periodo máximo permitido por la LPACAP (artículo 77.2).

Por otra parte, aunque la SEDIA y el MSND actúen para el cumplimiento de sus fines bajo el paraguas de la personalidad jurídica única de la AGE, ésta se organiza en Presidencia del Gobierno y en Ministerios, comprendiendo a cada uno de ellos uno o varios sectores funcionalmente homogéneos de actividad administrativa (artículo 57.1 LRJSP).

A su vez, cada Departamento Ministerial dispone de una estructura de órganos superiores y directivos prevista en el Real Decreto 139/2020, de 28 de enero, que asumen un determinado haz de competencias que será analizado en el FD VII.

La Sentencia del Tribunal Supremo (STS) 5298/1994, de 9 de julio de 1994, indica:

*"…la potestad sancionadora de la Administración goza de la misma naturaleza que la potestad penal, por lo que en consecuencia, las directrices estructurales del ilícito administrativo tienden también, como en el ilícito penal, a conseguir la individualización de la responsabilidad, vedando cualquier intento de construir una responsabilidad objetiva o basada en la simple relación con una cosa, por consiguiente en el ámbito de la **responsabilidad administrativa** no basta con que la conducta sea antijurídica y típica, sino que también es necesario que sea culpable, esto es, consecuencia de una acción u omisión **imputable a su autor** por malicia o imprudencia, negligencia o ignorancia inexcusable (STC, Sala del artículo 61 de la Ley Orgánica del Poder Judicial, de 6 de noviembre de 1990)"*

Por esta razón, aún actuando la SEDIA con personalidad jurídica única, según el principio de responsabilidad previsto en el artículo 28 de la LRJSP:

"Sólo podrán ser sancionadas por hechos constitutivos de infracción administrativa las personas físicas y jurídicas, así como, cuando una Ley les reconozca capacidad de obrar, los grupos de afectados, las uniones y entidades sin personalidad jurídica y los patrimonios independientes o autónomos, que resulten responsables de los mismos a título de dolo o culpa."

No obstante, el modo de atribución de responsabilidad a las personas jurídicas no se corresponde con las formas de culpabilidad dolosas o imprudentes que son imputables a la conducta humana. De modo que en el caso de infracciones cometidas por personas jurídicas, aunque haya de concurrir el elemento de la culpabilidad, éste se aplica necesariamente de forma distinta a como se hace respecto de las personas físicas.

Según la STC 246/1991 " (...) esta construcción distinta de la imputabilidad de la autoría de la infracción a la persona jurídica nace de la propia naturaleza de ficción jurídica a la que responden estos sujetos. Falta en ellos el elemento volitivo en sentido estricto, pero no la capacidad de infringir las normas a las que están sometidos.

Capacidad de infracción y, por ende, reprochabilidad directa que deriva del bien jurídico protegido por la norma que se infringe y la necesidad de que dicha protección sea realmente eficaz y por el riesgo que, en consecuencia, debe asumir la persona jurídica que está sujeta al cumplimiento de dicha norma" (en este sentido STS de 24 de noviembre de 2011, Rec 258/2009).

A lo expuesto debe añadirse, siguiendo la sentencia de 23 de enero de 1998, par-

cialmente trascrita en las SSTS de 9 de octubre de 2009, Rec 5285/2005, y de 23 de octubre de 2010, Rec 1067/2006, que "aunque la culpabilidad de la conducta debe también ser objeto de prueba, debe considerarse en orden a la asunción de la correspondiente carga, que ordinariamente los elementos volitivos y cognoscitivos necesarios para apreciar aquélla forman parte de la conducta típica probada, y que su exclusión requiere que se acredite la ausencia de tales elementos, o en su vertiente normativa, que se ha empleado la diligencia que era exigible por quien aduce su inexistencia; no basta, en suma, para la exculpación frente a un comportamiento típicamente antijurídico la invocación de la ausencia de culpa".

Respecto a los informes íntegros del Gabinete Jurídico que solicita, el informe 032/2020 fue enviado a la SEDIA el martes, 7 de abril de 2020 a las 22:56 vía correo electrónico e iba dirigido a:

Z.Z.Z. <EMAIL.1>;***

Y.Y.Y. <EMAIL.2>***

Con relación al informe 17/2020, está disponible en la página web de la AEPD: https://www.aepd.es/es/documento/2020-0017.pdf.

Por las consideraciones expuestas se desestiman las alegaciones aducidas."

Aún así, la SEDIA insiste en que, no se puede sostener la afirmación de la AEPD del FD IV de la Resolución recurrida, relativa a que las instrucciones dadas en las reuniones celebradas no eran suficientes para articular la relación entre responsable y encargado de tratamiento, ya que, la protección de la salud en un contexto de pandemia determinó la necesidad de actuar rápidamente de forma coordinada con la colaboración de todos los agentes implicados y la relación entre responsable y encargado de tratamiento se produjo de una manera más ágil, tal como exigían las circunstancias, pero no por ello, menos eficiente ni menos respetuosa con el derecho a la protección de datos de carácter personal ni el respeto al principio de seguridad jurídica.

En este sentido, en el FD X de la Resolución recurrida se decía:

"Remitámonos ahora, a la postura unívoca que hemos mantenido en los Informes del Gabinete Jurídico de la AEPD 17/2020 y 32/2020.

Para la AEPD "todo tratamiento de datos personales que deba realizarse como consecuencia de la pandemia y de la declaración del Estado de alarma deberá respetar el derecho fundamental a la protección de datos personales, ajustándose a las previsiones del RGPD, el cual permite… establecer reglas específicas respecto del ejercicio de dicho derecho, ajustado al propio RGPD, así como a la doctrina elaborada por el Tribunal Constitucional al interpretar el artículo 18.4 de nuestra Constitución, singularmente en lo relativo al principio de proporcionalidad…" .

Por tanto, de partida, no existe imposibilidad para armonizar los derechos e intereses de los usuarios, cuya protección exige escasa justificación ante la situación epidemiológica que aconteció."

Asimismo, la SEDIA insiste en que, en el proyecto piloto los datos no eran reales

(eran de prueba) y los códigos de contagiados para su introducción en la App eran falsos. Y que, cuando la App se abrió en La Gomera al público, las personas no podían introducir datos reales de estar infectados.

Pues bien, en el FD V de la Resolución recurrida, en base a los hechos probados, se determinó la existencia de un tratamiento de los datos personales de los usuarios de la aplicación, tanto en la fase del proyecto piloto como en la fase de la aplicación definitiva.

En este sentido, se indicó lo siguiente:

"Esta afirmación no contradice lo que se deduce de los hechos probados, pues el hecho de que la aplicación no solicitase datos personales que tuvieran que suministrarse por los usuarios, ni se les pidiera su nombre, número de teléfono o correo electrónico para poder crear un registro, no significa que no existiera un tratamiento de otros datos personales.

Que se tratasen datos personales pseudonimizados, tal y como también afirman, implica que hay tratamiento de datos personales.

Asimismo, el hecho de que en el proyecto piloto se trabajase con datos simulados de salud (falsos positivos) tal y como asevera la SEDIA en las alegaciones a la propuesta de resolución, no obsta para que sí se produjera el tratamiento de otros de los datos personales referenciados con anterioridad, máxime cuando los voluntarios se descargaron la aplicación en sus propios dispositivos móviles y desde los mismos reportaron los positivos.

Además, ha existido tratamiento de datos personales. Amén de los datos personales antes referidos y tratados en el proyecto piloto, la misma EIPD de agosto de 2020 concreta al examinar "todo el ciclo de vida y el flujo de los datos personales a través del tratamiento y todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin" respecto de la fase del ciclo de vida de los datos en que se produce la captura de los mismos que se produce con el "Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App", por parte de los usuarios del dispositivo móvil.

Esto significa que con la instalación de la aplicación ya se produce un tratamiento de datos personales.

Hay que destacar, en este momento, que el proyecto piloto no fue cerrado sólo a los voluntarios en el mismo, sino abierto a cualquiera que quisiera descargarse la aplicación.

La propia SEDIA afirma en el trámite de prueba que se producen los siguientes tratamientos, en concreto y tal y como consta en la política de privacidad de la aplicación,

"*La Secretaría General de Administración Digital, en calidad de titular de la aplicación y en base al encargo del tratamiento encomendado por el Ministerio de Sanidad, efectuará las siguientes operaciones del tratamiento:*

· Generación de códigos para la comunicación de positivos en la aplicación Ra-

dar COVID.

· Recepción de la información remitida por los usuarios cuando comunican un positivo. Las claves de exposición diaria hasta un máximo de 14 días. El número exacto de claves comunicadas dependerá de la fecha de inicio de síntomas o fecha de diagnóstico que se informa en la aplicación.

· Composición de un listado actualizado de claves de exposición temporal que son puestas a disposición para su descarga por parte de las aplicaciones Radar COVID".

(…)."

También insiste la SEDIA en que, ha quedado plenamente acreditado que en todo momento y de acuerdo con los instrumentos jurídicamente vinculantes, la SGAD actuó y actúa única y exclusivamente como encargada del tratamiento, mientras que el MSND y Comunidades Autónomas eran y son las responsables de dicho tratamiento.

Pues bien, estos roles fueron objeto de análisis en el FD VII de la resolución recurrida.

En este sentido, ya se indicó que:

"Aplicando lo anterior al caso que nos ocupa y como resultado de las actuaciones desarrolladas por el METD a través de la SEDIA y la SGAD, el papel que le correspondía a la SEDIA conforme al RGPD era el de encargado del tratamiento, ya que la competencia para el tratamiento de datos personales objeto de la aplicación desarrollada la tenía atribuida la actual Dirección General de Salud Pública (Real Decreto 735/2020, de 4 de agosto), antes, Dirección General de Salud Pública, Calidad e Innovación.

Sin embargo, de los hechos probados, se concluye que la SEDIA detentó la condición de responsable del tratamiento desde que se inició el proyecto en el mes de mayo de 2020, hasta el Acuerdo de uso de la aplicación "Radar COVID", en fase de pruebas, por parte de las Comunidades Autónomas y Ciudades Autónomas" de 19 de agosto de 2020 el Consejo Interterritorial del Sistema Nacional de Salud, antes citado, donde ya se reconoce a la SEDIA la condición de encargada del tratamiento.

Dicho lo anterior, y partiendo del hecho de que durante el proyecto piloto el responsable del tratamiento por ser titular de la competencia era la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad -admitido por la SEDIA en las alegaciones aducidas en el curso del procedimiento, indicando incluso que era encargada del tratamiento- lo cierto es que, considerando todas las circunstancias de hecho pertinentes y que han sido probadas, la SEDIA detentó la condición de responsable del tratamiento. Esta circunstancia ha quedado probada y deriva de la documentación que consta en el expediente administrativo y de las alegaciones formuladas durante el procedimiento sancionador.

Así, el rol de responsable del tratamiento que detentó la SEDIA, se pone de manifiesto a través de sus propias actuaciones tanto ad intra como ad extra.

Ad intra, respecto del resto de actores implicados en el proyecto piloto pertene-

cientes a la Administración Pública. La SEDIA determinó gran parte de los fines del tratamiento y decidió sobre los medios esenciales para llevarlo a término.

Hemos de partir de la carta de 9 de junio de 2020 de la Dirección General de Salud Pública, Calidad e Innovación. En dicha carta el responsable del tratamiento da el visto bueno al desarrollo del proyecto piloto Radar COVID mediante una aplicación móvil y también determina genéricamente la finalidad del tratamiento de datos personales en el citado proyecto piloto, esto es, la trazabilidad de contactos del COVID-19.

Aclaremos respecto a la alegación formulada por la SEDIA de que queda como encargada del tratamiento de los datos y resultados, que, la carta con relación a los roles se limita al siguiente tenor: "En su autorización la DGSP establece el 9 de junio de 2020 que: el responsable del tratamiento de los datos de este piloto será la autoridad sanitaria de la Comunidad en que se va a llevar a cabo".

Esta es una conclusión a la que parece, la SEDIA llega, a la vista de la investigación y posterior apertura del procedimiento sancionador: primero, porque la carta referenciada no hace mención al rol que ha de ocupar la SEDIA, sino que se limita a dar el visto bueno respecto del desarrollo del proyecto piloto; segundo, porque, si como entonces entendía la Dirección General de Salud Pública, Calidad e Innovación, el responsable del tratamiento era la autoridad sanitaria de la Comunidad Autónoma en la que se iba a llevar a cabo el tratamiento, a ella le hubiera correspondido designar al encargado del tratamiento a través de los instrumentos legalmente establecidos y no a la Dirección General de Salud Pública, Calidad e Innovación.

Sin perjuicio de que la Dirección General de Salud Pública, Calidad e Innovación, diera el visto bueno al proyecto piloto Radar COVID mediante la carta de 9 de junio de 2020, lo cierto es que no se determinó formalmente a la SEDIA como encargado del tratamiento durante el proyecto piloto.

Tampoco sirve a tales efectos la mención contenida respecto al "rol" de la SEDIA en el "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la COVID-19" de fecha 10 y 12 de junio de 2020, en la que se limitan a señalar que:

"La Orden SND/297/2020, de 27 de marzo, del Ministro de Sanidad encargó a la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA), del Ministerio de Asuntos Económicos y Transformación Digital, el desarrollo de diversas actuaciones para la gestión de la crisis sanitaria ocasionada por el COVID-19.

En particular, dicha Orden establece en su resolución primera, el Desarrollo de soluciones tecnológicas y aplicaciones móviles para la recopilación de datos con el fin de mejorar la eficiencia operativa de los servicios sanitarios, así como la mejor atención y accesibilidad por parte de los ciudadanos.

Adicionalmente, la Dirección General de Salud Pública, Calidad e Innovación, de la Secretaría General de Sanidad (Ministerio de Sanidad) ha dado el Visto Bueno a una prueba piloto de rastreo de contactos en relación a la COVID-19, encargan-

do a la SEDIA el desarrollo de una aplicación móvil para tal fin."

(…)

A lo anterior debemos añadir el documento denominado "COVID Radar. Secretaría General de Administración Digital. Funcionamiento general. Madrid, Junio 2020" donde la SEDIA informaba sobre los objetivos de la app:

"• Preservar la salud pública sin renunciar a la privacidad de los ciudadanos

• Ir un paso por delante del Covid-19: alertar a personas en riesgo es contener el virus de forma proactiva

• Minimizar el impacto económico del Covid-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas".

Así, la SEDIA al explicitar los objetivos de la aplicación, no estaba sino delimitando los fines del tratamiento, amplificando el fijado por la Dirección General de Salud Pública, Calidad e Innovación (la trazabilidad de contactos); esta participación en la determinación de las finalidades lleva implícita la condición de responsable del tratamiento.

Pero es que, además, determinó parte de los medios esenciales del tratamiento, decidiendo cuestiones tales como que, respecto de la interoperabilidad transfronteriza, se optase por el Protocolo DP3T descentralizado, que incorpora la API de Apple y Google o la propuesta de cinco modelos para la integración de la aplicación posterior en los servicios de salud autonómicos.

Igualmente, a través del "Pliego de condiciones para el diseño, desarrollo, piloto y evaluación de un sistema que permita el rastreo de contactos en relación con la pandemia ocasionada por la covid-19", aceptado por INDRA, se desarrollaron los medios del tratamiento previamente fijados. La "celebración" del contrato de emergencia con INDRA, como encargada de tratamiento, sin la consiguiente autorización del responsable real del tratamiento requerida por el artículo 28.2 del RGPD, pone de manifiesto que la SEDIA actuaba como responsable del tratamiento decidiendo sobre los medios del tratamiento.

También hay que citar el documento denominado "Diseño Piloto Covid-19 App. Presentación CCAA 17 junio 2020, elaborado por la SEDIA en el que se definen los parámetros clave del Piloto y los canales de acceso por los participantes.

Hay que añadir que, de toda la documentación obrante en el expediente administrativo no constan instrucciones documentadas del responsable real del tratamiento que justifiquen esta actuación "excesiva" de la SEDIA respecto de su rol de encargado del tratamiento.

Siguiendo con nuestra argumentación resulta muy significativa la versión inicial de la "Política de Privacidad de la Aplicación Radar COVID" publicada el día 7 de agosto de 2020 junto con la versión 1.0 de la app Radar COVID (versión piloto), donde consta la siguiente información:

"A tal efecto, utilizamos tus datos para prestarte el servicio de "Radar COVID" y para que puedas hacer uso de sus funcionalidades de acuerdo con sus condiciones de uso. De conformidad con el Reglamento General de Protección de Datos (RGPD) así como cualquier legislación nacional que resulte aplicable, ***la Secretaría General de Administración Digital tratará todos los datos generados durante el uso de la App para las siguientes finalidades****:*

Ofrecerte información sobre contactos considerados de riesgo de exposición a la COVID-19.

Proporcionarte consejos prácticos y recomendaciones de acciones a seguir según se produzcan situaciones de riesgo de cara a la cuarentena o auto-cuarentena.

Este tratamiento se llevará a cabo a través de la funcionalidad de alerta de contagios que permite identificar situaciones de riesgo por haber estado en contacto estrecho con personas usuarias de la aplicación que se encuentran infectadas por la COVID-19. De esta manera se te informará de las medidas que conviene adoptar después".

En esta información se asume con claridad el rol de responsable del tratamiento por la SGAD.

Asimismo, ad extra, a través de las notas de prensa publicadas por el METD, se pone de manifiesto que la SEDIA, desde un principio, actuó como responsable del tratamiento.

(…)

Como apuntábamos antes también se pronuncia respecto a los fines de la App que quedan vinculados a los fines del tratamiento en el siguiente sentido:

"La finalidad concreta del aplicativo de rastreo es cumplir con lo siguientes objetivos:

- *Preservar la salud pública sin renunciar a la privacidad de los ciudadanos.*
- *Ir un paso por delante de la COVID-19, alertando de forma proactiva a personas en riesgo de estar incubando el virus.*
- *Minimizar el impacto económico de la COVID-19, al controlar la pandemia sin medidas drásticas y facilitando el movimiento de personas."*

Y que duda cabe, con relación a la determinación de los medios, que es la SEDIA a través de la SGAD, la que ha desarrollado la aplicación de rastreo. Así se pone de manifiesto en la Resolución de 13 de octubre de 2020, de la Subsecretaría, que en su apartado Sexto dice:

"Que en aplicación de dichos principios, desde el mes de mayo de 2020, la SGAD ha venido desarrollando, con el conocimiento y la conformidad del Ministerio de Sanidad, una aplicación para la trazabilidad de contactos en relación a la pandemia ocasionada por la COVID-19 denominada «Radar COVID.

Durante el mes de julio de 2020, con la conformidad de la Dirección General de Salud Pública, Calidad e Innovación del Ministerio de Sanidad, la SGAD llevó a cabo con éxito el proyecto piloto de la misma, cuyo éxito garantiza la viabilidad de la solución propuesta para el rastreo de contactos estrechos."

Y aunque la SEDIA aduce que en todo momento estaban definidos los roles de responsable y encargado del tratamiento, y que sus actuaciones siempre han estado dirigidas a cumplir la función de encargada del tratamiento; o que la notas de prensa no pueden tener valor probatorio; o que el hecho de celebrar el "Acuerdo de contratación" no le atribuye el rol de encargado del tratamiento; así como que el MSND no estaba en condiciones de realizar la labor de difusión que realizó la SEDIA, lo cierto es que, en la resolución recurrida se consignan un total de 45 hechos probados, sin que esta Agencia pretenda extraer conclusiones y atribución de roles sin la correspondiente base probatoria.

La Agencia ya razonó en el FD IV de la Resolución recurrida los motivos por los que se incluían las notas de prensa en los hechos probados.

Subraya la SEDIA que el tratamiento de los datos por Radar Covid ha sido lícito refiriéndose a las bases de licitud del artículo 6 del RGPD en sus apartados d) y e).

Ciertamente, el Informe referido (17/2020), sin perjuicio de que pudieran existir otras bases, destacó que, el RGPD reconocía explícitamente las dos citadas: misión realizada en interés público (art. 6.1.e) o intereses vitales del interesado u otras personas físicas (art. 6.1.d).

Nada nuevo añade la SEDIA en las alegaciones formuladas en el recurso interpuesto respecto a la EIPD, más allá de insistir en que, la aplicación piloto utilizaba datos simulados, por lo que, si bien, la EIPD se hizo en un momento posterior a la puesta en funcionamiento del piloto, sí se hizo con anterioridad al momento en que la aplicación iba a manejar datos de salud reales de los usuarios. Nos remitimos a los FD V y X de la Resolución recurrida.

En cuanto a las condiciones de uso y política de privacidad, nada nuevo aduce la SEDIA. Insiste en que han estado siempre accesibles para los interesados, tanto desde la aplicación móvil, como desde la web http://radarcovid.gob.es y que, es necesario el consentimiento expreso del usuario para poder utilizar la aplicación, además de ser su uso totalmente voluntario. Pues bien, hay que señalar que, el artículo 12 del RGPD recoge las normas generales que deben observar los responsables al suministrar esta información, disponiendo, en su apartado 1, que el responsable del tratamiento debe facilitar a los interesados información concisa, transparente, inteligible y de fácil acceso sobre el tratamiento de sus datos personales, debiendo emplearse un leguaje claro y sencillo, en particular si la información se dirige específicamente a un niño. Se trata de facilitar la información de forma que los interesados entiendan lo que ocurrirá con sus datos. Los responsables del tratamiento deben facilitar la información de forma sucinta para evitar la fatiga informativa; en un lenguaje comprensible para un ciudadano medio; y de forma que sea fácilmente identificable que se está ofreciendo la información sobre protección de datos.

En el FD IX de la Resolución recurrida destacamos algunos de los aspectos controvertidos respecto a la información facilitada en las Condiciones de Uso y en la Política

de Privacidad, cuyo contenido se da por íntegramente reproducido.

Con relación las vulnerabilidades detectadas, nada nuevo argumenta. Nos remitimos a lo recogido en el FD XI de la Resolución recurrida.

Por último, respecto a la conclusión alcanzada: de que siempre actuó con responsabilidad proactiva, asumiendo el principio de privacidad desde el diseño, actuando en defensa del interés público en un contexto de estado de alarma que exigía celeridad y realizando las evaluaciones pertinentes, hay que señalar que, los hechos probados son constitutivos de las infracciones imputadas.

Nos reiteramos en que, la AEPD ha sido consciente de la situación extraordinaria y de emergencia que generó la pandemia del COVID conllevando la adopción de múltiples medidas para poner fin a la gravedad de la situación.

Es también evidente, que la privacidad, el derecho a la protección de los datos personales, no puede ser un obstáculo en los avances tecnológicos para combatir la pandemia. Como recoge el considerando 4 del RGPD: *el tratamiento de datos personales debe estar concebido para servir a la humanidad. El derecho a la protección de los datos personales no es un derecho absoluto, sino que debe considerarse en relación con su función en la sociedad y mantener el equilibrio con otros derechos fundamentales, con arreglo al principio de proporcionalidad.*

No obstante lo anterior, aún en ese contexto, no podemos obviar que la función primordial de la AEPD se refiere a la defensa efectiva del derecho fundamental a la protección de datos de carácter personal de la ciudadanía.

Respecto a lo solicitado por medio de Otrosí, respecto a la práctica de la prueba, como ya se indicó en la Resolución recurrida, destacar que, la SEDIA no formuló proposición de prueba alguna en el momento procedimental pertinente, a saber, su escrito de alegaciones presentado en fecha 22 de noviembre de 2021. También es preciso subrayar, que en el curso del procedimiento, la SEDIA ya se benefició de un período extraordinario de prueba por un plazo de diez días adicionales a los 30 inicialmente concedidos. Es decir, la práctica de prueba abarcó el periodo máximo permitido por la LPACAP (artículo 77.2). En suma, no ha lugar a la petición deducida.

En consecuencia y toda vez que, en el presente recurso de reposición, la SEDIA no ha aportado nuevos hechos o argumentos jurídicos que permitan reconsiderar la validez de la resolución impugnada.

Vistos los preceptos citados y demás de general aplicación, la Directora de la Agencia Española de Protección de Datos RESUELVE:

PRIMERO: DESESTIMAR el recurso de reposición interpuesto por la ***SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL*** contra la resolución de esta Agencia Española de Protección de Datos dictada con fecha 18 de febrero de 2022, en el procedimiento sancionador PS/00222/2021.

SEGUNDO: NOTIFICAR la presente resolución a la ***SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL***.

TERCERO: De conformidad con lo establecido en el artículo 50 de la LOPDGDD, la presente Resolución se hará pública una vez haya sido notificada a los interesados.

Contra esta resolución, que pone fin a la vía administrativa conforme al art. 48.6 de la LOPDGDD, y de acuerdo con lo establecido en el artículo 123 de la LPACAP, los interesados podrán interponer recurso contencioso-administrativo ante la Sala de lo Contencioso-administrativo de la Audiencia Nacional, con arreglo a lo dispuesto en el artículo 25 y en el apartado 5 de la disposición adicional cuarta de la Ley 29/1998, de 13 de julio, reguladora de la Jurisdicción Contencioso-administrativa, en el plazo de dos meses a contar desde el día siguiente a la notificación de este acto, según lo previsto en el artículo 46.1 de la referida Ley.

Finalmente, se señala que conforme a lo previsto en el art. 90.3 a) LPACAP, se podrá suspender cautelarmente la resolución firme en vía administrativa si el interesado manifiesta su intención de interponer recurso contencioso-administrativo. De ser éste el caso, el interesado deberá comunicar formalmente este hecho mediante escrito dirigido a la Agencia Española de Protección de Datos, presentándolo a través del Registro Electrónico de la Agencia [https://sedeagpd.gob.es/sede-electronica-web/], o a través de alguno de los restantes registros previstos en el art. 16.4 de la citada LPACAP. También deberá trasladar a la Agencia la documentación que acredite la interposición efectiva del recurso contencioso-administrativo. Si la Agencia no tuviese conocimiento de la interposición del recurso contencioso-administrativo en el plazo de dos meses desde el día siguiente a la notificación de la presente resolución, daría por finalizada la suspensión cautelar.

180-050422

Mar España Martí
Directora de la Agencia Española de Protección de Datos