GOBIERNO DE ESPAÑA
MINISTERIO DE ASUNTOS ECONÓMICOS Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO DE DIGITALIZACIÓN E INTELIGENCIA ARTIFICIAL

Radar COVID

Radar COVID
Informe de Evaluación de Impacto relativa a la Protección de Datos

Utilizando las últimas tecnologías para contener la pandemia Covid-19

Versión 2.0

4 de noviembre de 2020

Índice

1 INTRODUCCIÓN

1.1 Clasificación del Documento

Recomendamos la publicación de este documento en virtud de la Directriz 39 del documento "Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19", adoptadas el 21 de abril de 2020, por el Comité Europeo de Protección de Datos, donde se recomienda encarecidamente la publicación de la Evaluación de Impacto de Protección de Datos.

1.2 Objeto

La puesta en marcha de una política de protección de datos desde el diseño que incluya la realización de una Evaluación de Impacto relativa a la Protección de Datos resulta un elemento relevante a la hora de determinar la debida diligencia debida en la adopción de las necesarias garantías para el tratamiento de los datos.

El objetivo del presente documento es realizar la Evaluación del Impacto relativa a la Protección de los Datos (EIPD) del tratamiento llevado a cabo por la Aplicación "Radar COVID" (en adelante "la Aplicación", según lo exigido en el Reglamento (UE) 2016/679 del Parlamento Europeo (RGPD) cuando el tratamiento conlleve un alto riesgo para los derechos y libertades de las personas físicas. La EIPD es una herramienta preventiva, que ayuda a mitigar los riesgos antes de tratar datos personales, para que el tratamiento se realice con garantías de que se respetarán los derechos y libertades de los propietarios de los datos.

A lo largo del documento se describe la actividad de tratamiento, se justifica la necesidad y proporcionalidad del mismo y, por último, se presentan y analizan los resultados obtenidos con la herramienta de análisis de Riesgos PILAR (Procedimiento Informático-Lógico para el Análisis de Riesgos) desarrollada por Centro Criptológico Nacional (CCN) dependiente del Centro Nacional de Inteligencia (CNI). Estos resultados aportarán información respecto a los riesgos a los que está sometido el tratamiento, con su posterior mitigación mediante medidas técnicas y organizativas, incluyendo, en caso de ser necesario, un plan de tratamiento hasta conseguir llegar a un nivel de riesgo aceptable.

1.3 Consideraciones iniciales

La elaboración del presente informe sigue las directrices establecidas por la Agencia Española de Protección de Datos (en adelante "AEPD") en la "Guía práctica para las Evaluaciones de Impacto en la Protección de los Datos sujetas al RGPD". Por otro lado, la metodología utilizada para la realización de la evaluación sigue las fases y requisitos establecidos en el "Procedimiento de realización de EIPD" representado en el flujograma del apartado 1.5 del presente documento.

De acuerdo con lo anterior, el informe contiene la identificación del responsable del tratamiento. A su vez, se incluye una breve descripción del tratamiento, su finalidad, las principales categorías de datos destacando los factores de riesgo que motivan la realización de la presente EIPD. Se incluye también una breve descripción sobre el contexto de la EIPD, la extensión y límites de la misma, los principales riesgos de privacidad identificados, los beneficios del tratamiento y las soluciones de gestión planeadas.

1.4 Definiciones, acrónimos y expresiones

Las definiciones, acrónimos y expresiones relativas a los diferentes términos utilizados a lo largo del presente documento, pueden consultarse en el Anexo I**. Definiciones, acrónimos y expresiones.**

1.5 Flujograma del procedimiento de realización de EIPD

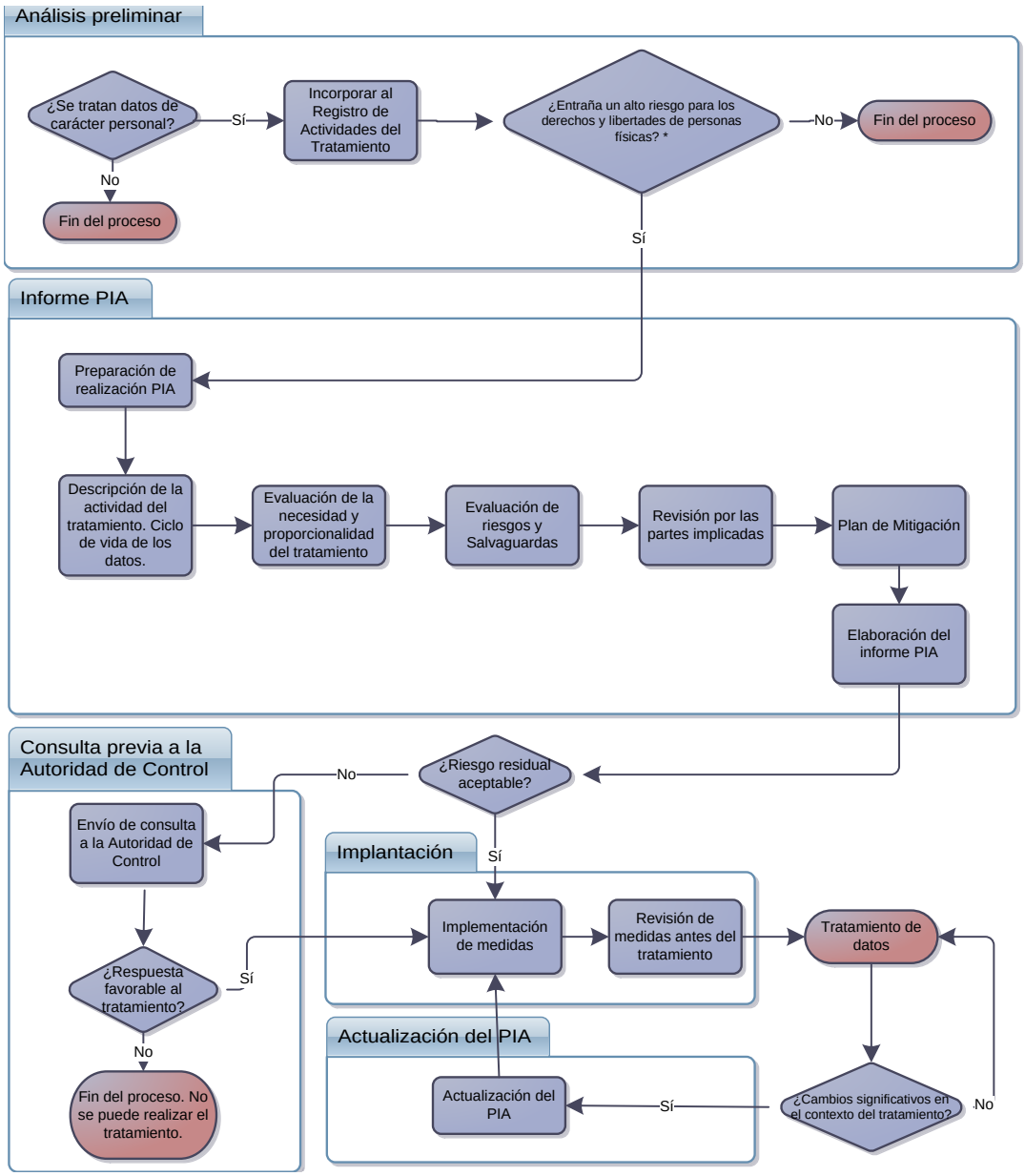

Ilustración 1. Flujograma del procedimiento

2 CARACTERIZACIÓN DEL TRATAMIENTO

2.1 Necesidad de realizar una EIPD

Antes de proceder a analizar si concurren los supuestos en los que la regulación establece que se debe realizar una EIPD, es importante poner de manifiesto la singularidad de este tratamiento en cuanto al tratamiento *sui generis* de datos de carácter personal.

Por defecto, los datos recopilados por la Aplicación no permiten la identificación directa del usuario o de su dispositivo, y son solo los necesarios para advertirle de que ha estado expuesto a un riesgo de contagio, 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.

Teniendo en cuenta esta premisa, se puede afirmar que estamos hablando de datos de personas que, aunque, por defecto, no permiten su identificación, sin embargo, pueden llegar a ser identificables.

Se entiende por dato de carácter personal «*cualquier información concerniente a personas físicas identificadas o identificables*». Una persona es **identificable** cuando su identidad pueda determinarse, **directa** o **indirectamente**, mediante un **identificador**, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, psíquica, económica, cultural o social, de dicha persona, salvo que dicha identificación requiera actividades o plazos desproporcionados.

Por tanto, se considera que una persona es identificada cuando la información disponible indica directamente a quién pertenece, sin necesidad de realizar una averiguación posterior. Por su parte, una persona es identificable cuando, aunque no haya sido identificada todavía, sea posible hacerlo.

En virtud de lo expuesto en el Considerando 30 del RGPD *«Las personas físicas pueden ser asociadas a identificadores en línea facilitados por sus dispositivos, aplicaciones, herramientas y protocolos, como direcciones de los protocolos de internet, identificadores de sesión en forma de "cookies" u otros identificadores, como etiquetas de identificación por radiofrecuencia. Esto puede dejar huellas que, en particular, al ser combinadas con identificadores únicos y otros datos recibidos por los servidores, pueden ser utilizadas para elaborar perfiles de las personas físicas e identificarlas».*

Por tanto, en los casos en que, a primera vista, la información no permite singularizar a una persona determinada, está 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.

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, la realización de una EIPD será preceptiva para la licitud del tratamiento.

El apartado 1 del artículo 35 establece, con carácter general, la obligación que tienen los responsables de los tratamientos de datos de realizar una EIPD con carácter previo a la puesta en funcionamiento de tales tratamientos cuando sea probable que estos por su naturaleza, alcance, contexto o fines entrañen un alto riesgo para los derechos y libertades de las personas físicas, alto riesgo que, según el propio Reglamento, se verá incrementado cuando los tratamientos se realicen utilizando «*nuevas tecnologías*».

Por otra parte, **el artículo 35.3 RGPD** establece que la EIPD se requerirá en particular en el caso de:

> a) *evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas físicas o que les afecten significativamente de modo similar*;
>
> b) *tratamiento a gran escala de las categorías especiales de datos a que se refiere el artículo 9, apartado 1, o de los datos personales relativos a condenas e infracciones penales a que se refiere el artículo 10, o*
>
> c) *observación sistemática a gran escala de una zona de acceso público*.

La AEPD ha publicado una lista de tipos de tratamientos de datos que requieren evaluación de impacto relativa a la protección de datos (artículo 35.4 RGPD).

Esta lista se basa en los criterios establecidos por el Grupo de Trabajo del Artículo 29 en la guía en la guía WP248 "*Directrices sobre la evaluación de impacto relativa a la protección de datos (EIPD) y para determinar si el tratamiento «entraña probablemente un alto riesgo» a efectos del RGPD*".

En el momento de analizar el tratamiento de datos será necesario realizar una EIPD en la mayoría de los casos en los que dicho tratamiento cumpla con dos o más criterios de la citada lista, salvo que el tratamiento se encuentre en la lista de tratamientos que no requieren EIPD a la que se refiere en artículo 35.5 del RGPD, que no es el caso de la actividad de tratamiento analizada.

Por ello, en base a la lista facilitada por la AEPD, debe considerarse que el tratamiento evaluado se identifica con los siguientes tratamientos incluidos en la citada lista:

> 1.- Tratamientos que impliquen el uso de datos a gran escala. Para determinar si un tratamiento se puede considerar a gran escala se considerarán los criterios establecidos en la guía WP243 "*Directrices sobre los delegados de protección de datos (DPD)*" del Grupo de Trabajo del Artículo 29.
>
> En este sentido y acudiendo a dicha guía, el Grupo de Trabajo recomienda que se tengan en cuenta los siguientes factores, en particular, a la hora de determinar si el tratamiento se realiza a gran escala:
>
> - el número de interesados afectados, bien como cifra concreta o como proporción de la población correspondiente;
> - el volumen de datos o la variedad de elementos de datos que son objeto de tratamiento;
> - la duración, o permanencia, de la actividad de tratamiento de datos;
> - el alcance geográfico de la actividad de tratamiento.
>
> Debe tenerse en cuenta, como ya se ha apuntado anteriormente, que el tratamiento de la información, en este caso, no solo afecta al usuario de la Aplicación sino también a la de todos los terceros con los que ha estado en contacto.
>
> 2.- Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.
>
> En el caso de las aplicaciones de rastreo de contactos, se produce un seguimiento sistemático y masivo de los contactos de las personas físicas, lo que podría suponer una grave injerencia en su privacidad.
>
> 3. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD.
>
> En este sentido, es importante tener en cuenta que el tratamiento no sólo implica un tratamiento de datos a gran escala, sino un tratamiento a gran escala de categorías especiales de datos (datos relativos a la salud).

Según el artículo 4, apartado 15, del RGPD, por «*datos relativos a la salud*» se entenderá los datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud, concepto que viene derivado del Apartado 45 de la Memoria Explicativa del Convenio 108 del Consejo de Europa.

Como se indica en el considerando 53, los datos relativos a la salud merecen una mayor protección, pues el uso de esos datos sensibles puede tener repercusiones negativas significativas para los interesados. A la luz de lo anterior y de la jurisprudencia pertinente del Tribunal de Justicia de la Unión Europea el término «*datos relativos a la salud*» debe interpretarse en sentido amplio.

El respeto al carácter confidencial de la información sobra la salud, constituye un principio esencial del sistema jurídico de los estados, donde con su regulación interna prevé garantías apropiadas para impedir toda comunicación o divulgación de datos relativos a la salud, contra las garantías previstas en el artículo 8 del Convenio Europeo de Derechos Humanos y nuestra normativa sobre Privacidad.

Los datos relativos a la salud pueden obtenerse de diversas fuentes, por ejemplo:

a. Información recopilada por un proveedor de asistencia sanitaria en un historial médico (por ejemplo, historia clínica y resultados de exámenes y tratamientos).

b. Información que se convierte en datos sanitarios al ser objeto de referencia cruzada con otros datos, por lo que revela el estado de salud o los riesgos para la salud (como la suposición de que una persona presenta un mayor riesgo de sufrir ataques cardiacos basada en la medición de una presión arterial elevada durante un determinado período de tiempo).

c. Información procedente de una encuesta de «*autocomprobación*», en la que los interesados responden a preguntas relacionadas con su salud (por ejemplo, declaración de síntomas).

d. Información que se convierte en datos sanitarios al ser utilizada en un contexto específico (por ejemplo, información sobre un viaje reciente o la presencia en una región afectada por la COVID-19 tratada por un profesional médico para realizar un diagnóstico).

4. Tratamientos que impliquen la utilización de nuevas tecnologías o un uso innovador de tecnologías consolidadas, incluyendo la utilización de tecnologías a una nueva escala, con un nuevo objetivo o combinadas con otras, de forma que suponga nuevas formas de recogida y utilización de datos con riesgo para los derechos y libertades de las personas.

Esta Aplicación usa la tecnología Bluetooth de los teléfonos móviles que permite la conexión con aparatos cercanos como auriculares, altavoces o relojes.

Por último y en virtud de lo previsto en las **Directrices 04/2020 sobre el uso de datos de localización y herramientas de rastreo de contactos en el contexto de la pandemia de COVID-19, adoptadas el 21 de abril de 2020, el Comité Europeo de Protección de Datos** coincide en que ha de llevarse a cabo una Evaluación de Impacto relativa a la Protección de Datos (EIPD) antes de empezar a utilizar una Aplicación de este tipo por cuanto se considera que el tratamiento puede entrañar un alto riesgo:

- Datos sanitarios,
- Adopción previa a gran escala,
- Seguimiento sistemático,
- Utilización de una nueva solución tecnológica,

Por todo ello, en el tratamiento evaluado, **concurren factores que contribuyen a generar un nivel de riesgo elevado, debiéndose realizar una EIPD al objeto de determinar un escenario de gestión del riesgo adecuado.**

2.2 Responsables, corresponsables y encargados del tratamiento

El artículo 4 del RGPD define como responsable del tratamiento: *la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros* (corresponsabilidad) *determine los fines y medios del tratamiento*.

Podemos decir que la definición se compone de tres elementos fundamentales: (i) el aspecto personal (la persona física o jurídica, autoridad pública, servicio u otro organismo); (ii) la posibilidad de un control plural (que solo o conjuntamente con otros); y (iii) los elementos esenciales para distinguir al responsable del tratamiento de otros agentes (determinación de los fines y los medios de tratamiento).

En relación con la determinación de los fines y los medios. El hecho de determinar los fines trae consigo la consideración de facto de responsable del tratamiento. Es sin embargo en la determinación de los medios de procesamiento, lo que puede ser delegado sobre un tercero y adquirir éste la condición de encargado de tratamiento.

Con fecha 10 de junio de 2020, se publicó en el Boletín Oficial del Estado (BOE), el 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, cuyo objetivo es la adopción de una serie de medidas urgentes de prevención, contención y coordinación, dirigidas a garantizar el derecho a la vida y a la protección de salud mientras perdure la crisis sanitaria ocasionada por el COVID-19, una vez expirada la vigencia del estado de alarma y de las medidas extraordinarias de contención, incluidas las restrictivas de la libertad de circulación, establecidas al amparo de aquel.

En el artículo 5 del citado Real Decreto-Ley, "*Planes y estrategias de actuación para afrontar emergencias sanitarias",* se establece lo siguiente:

> «*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».*

Asimismo, en el Artículo 26 del mismo Real Decreto-Ley*, "Provisión de información esencial para la trazabilidad de contactos",* se dispone lo siguiente:

> *«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».*

Por otro lado, en el artículo 27.2 de dicha norma, se establece que la finalidad del tratamiento de la información de carácter personal que se realice como consecuencia del desarrollo y Aplicación de dicha norma será 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.

El desarrollo de la Aplicación se puede incluir, por tanto, en el plan de actuación para afrontar las emergencias sanitarias y prevenir y evitar situaciones excepcionales de especial gravedad y por tanto quedaría bajo el marco legal de este Real Decreto-Ley.

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.

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.

2.3 Descripción del tratamiento. Ciclo de vida de los datos

A continuación, se realiza la descripción del tratamiento y del ciclo de vida de los datos.

2.3.1 Nombre y descripción del tratamiento

La presente evaluación se realiza sobre el tratamiento de datos personales que se lleva a cabo en la Aplicación. El tratamiento se va a llevar a cabo a través una Aplicación de rastreo de contactos que ayude a los ciudadanos a descubrir si han estado en contacto con una persona infectada por el SARS-CoV-2. El objetivo del tratamiento es que las personas que hayan estado cerca de alguien que resulte ser portador confirmado del virus sean informadas de ello, a fin de romper las cadenas de transmisión de la enfermedad lo antes posible. Además, la Aplicación proporciona consejos sobre prevención de contagio y qué hacer si desarrollan síntomas.

2.3.2 Datos personales objeto del tratamiento

Los datos recopilados y generados por la Aplicación no permiten, por defecto, la identificación directa del usuario o de su dispositivo, y son solo los necesarios para advertirle de que ha estado expuesto a un riesgo de contagio, 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.

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 Aplicación 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 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 a los usuarios de la aplicación mediante *Quick Response code* (QR). Los usuarios podrán, voluntariamente, introducir dicho código en la Aplicación para confirmar el diagnóstico positivo y desencadenar el procedimiento de notificación a sus contactos estrechos. Este código es una confirmación de diagnóstico positivo de un usuario. Existe verificación de dicho código para evitar que cualquier usuario envíe pruebas 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.

Sin perjuicio de lo anterior, estos datos no permiten la identificación directa del usuario o de su dispositivo, existiendo estudios sobre la robustez de los protocolos de criptografía y anonimización, aunque existe la posibilidad de que puedan romperse y asociarse los identificadores con números de teléfono y personas, aplicando suficiente tiempo y capacidad de cómputo, si bien esto se considera altamente improbable. Por otra

parte, debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la aplicación, sino también la de todos los terceros con los que ha estado en contacto.

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*, o 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).

2.3.3 Finalidad del tratamiento

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.
- Los datos también podrán ser procesados fines de investigación científica o fines estadísticos. En tal caso los datos se encontrarán totalmente anonimizados.

2.3.4 Análisis del tratamiento

Como punto de partida, es necesario conocer en detalle todo el ciclo de vida y el flujo de los datos personales a través del tratamiento, así como todos los actores y elementos que intervienen durante las actividades de tratamiento desde su inicio hasta su fin.

El apartado a) del artículo 35.7 del RGPD establece la obligación de que la EIPD incluya, al menos, una descripción sistemática y detallada del tratamiento. Adicionalmente a la descripción del tratamiento, se debe obtener una descripción clara de los elementos que intervienen en cada una de las fases del ciclo de vida de los datos del tratamiento.

Fase del ciclo de vida de los datos	Actividad	Actores	Sistemas
Captura de datos	• Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App.	Usuarios	Dispositivo móvil
Almacenamiento	• Generación de códigos aleatorios: Se generan en el back-end del sistema y se ponen a disposición de las CCAA a través de un servicio Web. Todo esto está en los servidores del cloud AWS (Amazon Web Services).		
	• Compartición por Bluetooth (BT): a través de BT se realiza el intercambio de identificadores aleatorios y sólo entre terminales móviles.	Usuarios	Dispositivo móvil
	• Registro de códigos anónimos de otros usuarios que también tienen instalada la App • Recolectar las balizas de los usuarios que hayan sido diagnosticados de Covid-19	Administradores de Amazon	Servidor externo: Servidor de Amazon.
Uso y tratamiento	• Las autoridades sanitarias entregan el código de positivo a un usuario con PCR positiva que lo introduce en el dispositivo móvil.	Autoridades sanitarias	Servicios Autonómicos de Salud
	• Cuando una persona es positiva se suben sus claves al servidor central para distribuir a los terminales y que cada terminal analice (en local) el nivel de riesgo con respecto a esas claves infectadas. • Se activa el mecanismo de seguimiento de contactos y se envían notificaciones a usuarios en riesgo.		Servidores de AWS
Cesiones	• Integración con otros sistemas de la Unión Europea (no hay transferencia internacional de datos).	La Comisión Europea	Pasarela Federativa
Destrucción	• Destrucción de la información transcurridos los plazos legales de conservación de la información, una vez han dejado de servir a la finalidad para la que fueron recogidos (14 días). • Cuando se declare fin de la pandemia por la OMS y esto se refleje por parte de las autoridades sanitarias competentes por los cauces normativos que sean oportunos, debe establecerse un procedimiento para detener la recogida de identificadores (desactivación global de la aplicación, instrucciones para desinstalarla, desinstalación automática, etc.) y para activar la eliminación de todos los datos recogidos de todas las bases de datos (aplicaciones móviles y	Usuarios	Desinstalación de la App
		Administradores de Amazon Autoridades sanitarias	Datos en servidores de Amazon y datos en servidor central No definido

	Servidores).		

Tabla 1. Tabla resumen. Fases del ciclo de vida de los datos

2.3.5 Tecnologías intervinientes

La Aplicación ha sido desarrollada por la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA). Esta Aplicación no recoge ni trata, por defecto, datos que puedan identificar directamente al usuario del dispositivo. Los datos que se almacenan se generan como consecuencia del funcionamiento de la Aplicación y para cumplir con la finalidad de la aplicación. Se alojan en un servidor central en el que se gestionan dichos datos traducidos en las balizas de los usuarios que han sido diagnosticados de COVID-19. Desde este servidor se distribuyen a los dispositivos de los usuarios que han estado en contacto, las balizas de los confirmados.

La Aplicación ha sido desarrollada en estrecha colaboración con los fabricantes de los sistemas operativos, en este caso Google y Apple, ya que el acceso y el tratamiento de los datos por la Aplicación se gestionan mediante una API integrada en el sistema operativo.

A efectos de medir la proximidad y estimar los contactos estrechos, se produce una comunicación entre dispositivos por Bluetooth de baja energía (BLE) que parece ser más precisa y, por tanto, más apropiada que la utilización de los datos de geolocalización (GNSS/GPS o datos de localización de dispositivos móviles). Además, el BLE no permite la geolocalización.

La Aplicación debe comunicarse con un servidor externo que provee un código de autorización que confirme el positivo y pueda autorizar a subir las balizas al servicio, en función del siguiente ciclo propuesto:

- Sistema médico solicita token/QR autenticación al back-end para confirmar positivo COVID-19.
- Paciente recibe token/QR autenticación para confirmar el positivo COVID-19.
- Paciente envía el token/QR autorizado al back-end para subir su histórico de contactos.

2.3.6 Licitud del tratamiento y cumplimiento normativo

a). - Legitimación

i). - <u>Instalación de las aplicaciones y almacenamiento de información en el dispositivo del usuario</u>

En virtud de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (artículo 5), el almacenamiento de información en el dispositivo del usuario o la obtención de acceso a la información ya almacenada se permite únicamente si: i) el usuario ha dado su consentimiento, o ii) el almacenamiento o el acceso son estrictamente necesarios para el servicio de la sociedad de la información, en este caso la Aplicación, que el usuario ha solicitado de manera expresa (esto es, mediante la instalación y activación).

En el caso de la Aplicación objeto de evaluación, no se cumple el requisito ii), ya que la carga de datos de proximidad para el rastreo de contactos y alerta no es necesaria para el funcionamiento de la Aplicación en sí misma, por tanto, **es necesario obtener el consentimiento** libre, específico, explícito e informado, mediante una clara acción afirmativa del usuario.

<u>ii). - Base jurídica para el tratamiento por parte de las autoridades sanitarias nacionales (Derecho de la Unión o de un Estado miembro)</u>

El Considerando (46) del RGPD reconoce que en situaciones excepcionales tales como una epidemia, la base jurídica de los tratamientos puede ser múltiple, **basada tanto en el interés público, como en el interés vital del interesado u otra persona física.**

> *« (46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios, incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano».*

Por tanto, como base jurídica para un tratamiento lícito de datos personales, el RGPD reconoce 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).**

El art. 6.1, letra d) RGPD considera no sólo que el interés vital es suficiente base jurídica del tratamiento para proteger al «interesado» (en cuanto que este es un término definido en el art. 4.1) RGPD como persona física identificada o identificable), sino que dicha base jurídica puede ser utilizada para proteger los intereses vitales «de otra persona física», lo que por extensión supone que dichas personas físicas pueden ser incluso no identificadas o identificables; es decir, dicha base jurídica del tratamiento (el «interés vital») puede ser suficiente para los tratamientos de datos personales dirigidos a proteger a todas aquellas personas susceptibles de ser contagiadas en la propagación de una epidemia, lo que justificaría, desde el punto de vista de tratamiento de datos personales, en la manera más amplia posible, las medidas adoptadas a dicho fin, incluso aunque se dirijan a proteger personas innominadas o en principio no identificadas o identificables, por cuanto los intereses vitales de dichas personas físicas habrán de ser salvaguardados, y ello es reconocido por la normativa de protección de datos personales.

El apartado 3 del artículo 6 RGPD no establece la necesidad de que la base del tratamiento por razón de interés vital haya de ser establecida por el Derecho de la Unión o el Derecho de los Estados Miembros aplicables al responsable del tratamiento, pues dicho apartado se refiere exclusivamente a los tratamientos establecidos para el cumplimiento de una obligación legal, o para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos, ambas referidas en las letras c) y e) de dicho artículo 6 RGPD, pero no para los tratamientos incluidos en la letra d).

iii).- Sin embargo, **para el tratamiento de datos de salud** no basta con que exista una base jurídica del art. 6 RGPD, sino que de acuerdo con el art. 9.1 y 9.2 RGPD exista una circunstancia que levante la prohibición de tratamiento de dicha categoría especial de datos (entre ellos, datos de salud).

LA AEPD entiende que dichas circunstancias cabe encontrarlas, en este caso, en varios de los epígrafes del **art. 9.2 RGPD**. Así:

- En la letra g), y en la i), que pueden ser examinadas conjuntamente, por cuanto ambas hacen referencia a un interés público, el primero de ellos calificado de «*esencial*» y el segundo de ellos que hace referencia a un interés público calificado «*en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud*», todo ello sobre la base del Derecho de la Unión o de los Estados Miembros que establezca medidas adecuadas y específicas para proteger los derechos y libertades del interesado, en particular el secreto profesional.
- En la letra h), cuando el tratamiento es necesario para realizar un diagnóstico médico, o evaluación de la capacidad laboral del trabajador o cualquier otro tipo de asistencia de tipo sanitario o para la gestión de los sistemas y servicios de asistencia sanitaria y social.
- Una última circunstancia de cierre que permitiría el tratamiento de datos de salud podría ser incluso la establecida en la letra c), en el caso de que se den las circunstancias previstas en este apartado, que aplicaría cuando el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física, en el supuesto de que el interesado no esté capacitado, física o jurídicamente, para dar su consentimiento.

En consecuencia, en una situación de emergencia sanitaria, como es el caso, es preciso tener en cuenta que, en el exclusivo ámbito de la normativa de protección de datos personales, la Aplicación de la normativa de

protección de datos personales permitiría adoptar al responsable del tratamiento aquellas decisiones que sean necesarias para salvaguardar los intereses vitales de las personas físicas, el cumplimiento de obligaciones legales o la salvaguardia de intereses esenciales en el ámbito de la salud pública, dentro de lo establecido por la normativa material aplicable.

Por ello, el responsable de la aplicación, al estar actuando para salvaguardar dichos intereses, deberá actuar conforme a lo que las autoridades establecidas en la normativa del Estado miembro correspondiente, en este caso España, establezcan.

En materia de riesgo de transmisión de enfermedades, epidemia, crisis sanitarias etc., la normativa aplicable ha otorgado «a las autoridades sanitarias de las distintas Administraciones públicas» (art. 1 Ley Orgánica 3/1986, de 14 de abril) las competencias para adoptar las medidas necesarias previstas en dichas leyes cuando así lo exijan razones sanitarias de urgencia o necesidad.

En consecuencia, desde un punto de vista de tratamiento de datos personales, la salvaguarda de intereses esenciales en el ámbito de la salud pública corresponde a las distintas autoridades sanitarias de las diferentes administraciones públicas, quienes podrán adoptar las medidas necesarias para salvaguardar dichos intereses esenciales públicos en situaciones de emergencia sanitaria de salud pública.

Serán estas autoridades sanitarias competentes de las distintas administraciones públicas quienes deberán adoptar las decisiones necesarias, y los distintos responsables de los tratamientos de datos personales deberán seguir dichas instrucciones, incluso cuando ello suponga un tratamiento de datos personales de salud de personas físicas. Lo anterior hace referencia, expresamente, a la posibilidad de tratar los datos personales de salud de determinadas personas físicas por los responsable de tratamientos de datos personales, cuando, por indicación de las autoridades sanitarias competentes, es necesario comunicar a otras personas con las que dicha persona física ha estado en contacto la circunstancia del contagio de esta, para salvaguardar tanto a dichas personas físicas de la posibilidad de contagio (intereses vitales de las mismas) cuanto para evitar que dichas personas físicas, por desconocimiento de su contacto con un contagiado puedan expandir la enfermedad a otros terceros (intereses vitales de terceros e interés público esencial y/o cualificado en el ámbito de la salud pública).

iv).- Se enumera, a continuación la legislación aplicable:

- 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
- Decreto-ley, de 9 de junio, tiene por objeto establecer las medidas urgentes de prevención, contención y coordinación necesarias para hacer frente a la crisis sanitaria ocasionada por el COVID-19, así como prevenir posibles rebrotes, con vistas a la superación de la fase III del Plan para la Transición hacia una Nueva Normalidad por parte de algunas provincias, islas y unidades territoriales y, eventualmente, la expiración de la vigencia del estado de alarma declarado por 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, y sus prórrogas.
- Decisión de Ejecución (UE) 2020/1023 de la Comisión de 15 de julio de 2020 que modifica la Decisión de Ejecución (UE) 2019/1765 en lo concerniente al intercambio transfronterizo de datos entre las aplicaciones móviles nacionales de rastreo de contactos y advertencia para combatir la pandemia de COVID-19

2.3.7 Análisis de la necesidad, proporcionalidad del tratamiento

El principio de «*minimización de datos*» establece que los datos personales serán «*adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que serán tratados*». Durante la definición del mismo, se debe considerar qué datos son estrictamente necesarios para realizar las actividades de tratamiento en función de las finalidades previstas.

La proporcionalidad tiene que ver con evaluar si la finalidad que se persigue se puede conseguir por otros medios, por ejemplo: utilizando otros datos, reduciendo el universo de personas afectadas (de manera cuantitativa o cualitativa), haciendo uso de otras tecnologías menos invasivas o bien aplicando otros procedimientos o medios de tratamiento (modificando los inicialmente previstos), etc.

Para comprobar si el tratamiento supone una medida restrictiva de un derecho fundamental, este debe superar los tres puntos del llamado juicio de proporcionalidad:

- Juicio de idoneidad: si la medida puede conseguir el objetivo propuesto.
- Juicio de necesidad: si, además, es necesario, en el sentido de que no existe otra más moderada para conseguir este propósito con la misma eficacia.
- Juicio de proporcionalidad en sentido estricto: si la medida es ponderada o equilibrada, porque se derivan más beneficios o ventajas para el interés general que no perjuicios sobre otros bienes o valores en conflicto.

i). - **Juicio de Proporcionalidad:** Es necesario determinar y justificar que el tratamiento es proporcional, asegurando que se cumplen los siguientes principios:

- **Principio de limitación de la finalidad**: los datos serán recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines de conformidad con el artículo 5, apartado 1, letra b), del RGPD.

  No obstante, según la «*presunción de compatibilidad*» prevista en el artículo 5, apartado 1, letra b), del RGPD, de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de [...] investigación científica [...] no se considerará incompatible con los fines iniciales.

  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 diagnósticas correspondientes.

  Esto es, pues, útil tanto para los ciudadanos como para las autoridades sanitarias públicas. También puede desempeñar un papel importante en la gestión de las medidas de confinamiento durante las posibles situaciones de desescalada.

  No obstante, la Aplicación contiende varias funcionalidades y cada una de las distintas funcionalidades de la Aplicación obedece a determinados fines:

  • 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.

- **Principio de minimización de datos:** el principio de minimización de datos exige que únicamente se traten los datos personales que sean adecuados, pertinentes y estrictamente necesarios en relación con los fines por los que se lleva a cabo el tratamiento. En vista del

fin o los fines perseguidos, se lleva a cabo una valoración de la necesidad de tratar los datos personales y la pertinencia de tales datos personales.

Se puede concluir que se recaban exclusivamente los datos personales que se requieren para las finalidades indicadas.

En relación con la finalidad de rastreo de contactos y alerta, se tratan datos de proximidad, a través de la comunicación de dispositivos por Bluetooth de baja energía (BLE) que no permiten la geolocalización, por lo que no se utilizan datos de localización.

Por otro lado, no se lleva a cabo el almacenamiento, ni el momento exacto, ni el lugar de contacto. Sin embargo, sí parece útil almacenar el día del contacto, para saber si se produjo cuando la persona experimentaba síntomas (o cuarenta y ocho horas antes) y definir con mayor precisión el mensaje de seguimiento en el que se ofrezcan consejos relacionados, por ejemplo, con la duración de la auto cuarentena.

- **Principio de limitación del plazo de conservación**: El principio de limitación del almacenamiento exige que los datos no se conserven durante más tiempo del necesario.

  Los plazos se basan en la importancia médica y en lapsos realistas para las medidas administrativas que, si procede, deban tomarse.

  - Los datos generados para el rastreo de contactos y alerta: Los datos de proximidad se suprimirán tan pronto como dejen de ser necesarios para alertar a las personas y como máximo tras un período de un mes (período de incubación más el margen).

    Los datos se almacenan en el dispositivo del usuario, y solo aquellos que hayan sido comunicados por los usuarios y que sean necesarios para cumplir la finalidad se cargan en el servidor central de validación de positivos a disposición de las autoridades sanitarias cuando se haya elegido tal opción (es decir, solo se cargarían los datos en el servidor de «*contactos estrechos*» de una persona que hubiera dado positivo a la infección de COVID-19).
    En todo caso, los datos personales solo deben conservarse durante la crisis de la COVID-19. Después, como regla general, todos los datos personales deberían borrarse o anonimizarse.

ii). - **Necesidad; se trata de comprobar si la medida es necesaria, en el sentido de que no exista otra más moderada para la consecución de tal propósito con igual eficacia.**

Es muy importante considerar la utilidad real, la necesidad y efectividad de esta Aplicación, así como su impacto en el sistema social más amplio, incluidos los derechos fundamentales y libertades, considerando que estas aplicaciones sientan un precedente para el uso futuro de tecnologías invasivas similares, incluso después de la crisis COVID-19.

La situación de emergencia no puede suponer una suspensión del derecho fundamental a la protección de datos personales. Pero, al mismo tiempo, la normativa de protección de datos no puede utilizarse para obstaculizar o limitar la efectividad de las medidas que adopten las autoridades competentes, especialmente las sanitarias, en la lucha contra la epidemia, ya que en ella se prevén soluciones que permiten compatibilizar el uso lícito de los datos personales con las medidas necesarias para garantizar eficazmente el bien común.

Como ya se ha comentado anteriormente, los fundamentos que legitiman/hacen posible dichos tratamientos son la necesidad de atender las misiones realizadas en interés público, así como la de garantizar los intereses vitales de los propios afectados o de terceras personas, en virtud de lo expuesto en el Considerando 46 del RGPD, donde se reconoce que en situaciones excepcionales, como una epidemia, la base jurídica de los tratamientos puede ser múltiple, basada tanto en el interés público, como en el interés vital del interesado u otra persona física.

> *« (46) El tratamiento de datos personales también debe considerarse lícito cuando sea necesario para proteger un interés esencial para la vida del interesado o la de otra persona física. En principio, los datos personales únicamente deben tratarse sobre la base del interés vital de otra persona física cuando el tratamiento no pueda basarse manifiestamente en una base jurídica diferente. Ciertos tipos de tratamiento pueden responder tanto a motivos importantes de interés público como a los intereses vitales del interesado, como por ejemplo cuando el tratamiento es necesario para fines humanitarios,*

incluido el control de epidemias y su propagación, o en situaciones de emergencia humanitaria, sobre todo en caso de catástrofes naturales o de origen humano».

Por tanto, si procedemos a realizar un juicio de necesidad, es decir, determinar si el tratamiento es necesario, en el sentido de que no existe otra alternativa menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable, conviene apuntar que la legislación sectorial en materia sanitaria no cuenta en la actualidad con instrumentos suficientemente precisos que permitieran afrontar una situación como la de crisis sanitaria en la que el país aún se encuentra inmerso.

En este sentido, se han aprobado medidas específicas, como es el desarrollo de una Aplicación como la que se está evaluando, que refuerzan los instrumentos de coordinación y cooperación en materia de salud pública a la vista de las características globales de la epidemia.

La experiencia vivida durante la crisis sanitaria ha puesto de relieve la perentoriedad del suministro de información entre autoridades sanitarias que facilite el seguimiento de la evolución epidemiológica y de las medidas de prevención, control y contención adoptadas al respecto.

iii). - **Proporcionalidad en sentido estricto: se trata de comprobar si la medida es ponderada o equilibrada por derivarse de ella más beneficios o ventajas para el interés general que perjuicios sobre otros bienes o valores en conflicto.**

En este caso, el beneficio tendrá que medirse en función de una menor propagación de la infección en términos globales, con la posibilidad de recuperar la libertad de acción, y una protección de la salud de los individuos. Los datos de salud tienen un alto valor, por lo que hay que prevenir que, aprovechando la incertidumbre que provoca una situación de emergencia, se produzcan abusos por parte de terceros que conduzcan a situaciones de pérdida de libertades, discriminación u otros daños en la situación personal de los ciudadanos.

Se trata por tanto de realizar una valoración de los beneficios que este tratamiento promete aportar en la lucha frente a la pandemia y de los costes en la privacidad de los individuos que pueden acarrear.

En cuanto a los posibles perjuicios o amenazas que puede suponer una Aplicación como esta para la privacidad:

Habrá que tener en cuenta cómo se ha realizado la Aplicación que estamos evaluando y de cuáles son sus objetivos. Estas amenazas pueden aparecer por la urgencia en ofrecer soluciones en funcionamiento que relajen los controles y requisitos para proteger los datos de los ciudadanos. Por ejemplo, se pueden encontrar posibles amenazas a la privacidad en la implementación de la misma. Por otra parte, no hay que olvidar que una app o una web es solamente un interfaz para mostrar y llevar datos a un servidor.

Las principales amenazas a la privacidad de este tipo de soluciones vienen de la realización de mapas de relaciones entre personas, re-identificación por localización implícita, de la fragilidad de los protocolos a la hora construir «*tarjetas*» casi anónimas, y de dispersar las señales de los contagios de forma que no se identifique en ningún caso la identidad de los contagiados. Debe tenerse en cuenta que el tratamiento de la información no solo afecta al usuario de la Aplicación sino también la de todos los terceros con los que ha estado en contacto, por lo que este tratamiento ha de cumplir los principios de protección de datos.

Hay estudios sobre la robustez de los protocolos de criptografía y anonimización y siempre existe una posibilidad de que aplicando suficiente tiempo y capacidad de cómputo puedan romperse y asociar los apodos anónimos con números de teléfono y personas. Desde el punto de vista de la privacidad, cuanto más cálculo se haga en la parte de servidor, menos control tienen los usuarios, por lo que las soluciones centralizadas siempre parecen menos respetuosas con la privacidad que las distribuidas. La posibilidad de que, debido a la acumulación de los datos de forma centralizada, se produjese un abuso en una empresa poco ética, se ampliarán los propósitos del tratamiento o se fuera víctima de un ciberataque constituye otra de las mayores amenazas de este tipo de soluciones.

En cuanto los beneficios que puede representar este tipo de tratamiento, es importante traer a colación, el análisis realizado por la AEPD sobre si el uso de estos datos representa en la crisis de la pandemia un beneficio importante, determinando que el éxito de este tipo de soluciones se basa en muchos factores que no dependen de la tecnología. En primer lugar, es necesaria la implicación de un elevado número de usuarios, algunos estudios hablan de al menos el 60% de una población que, teniendo en cuenta a los niños y los ancianos, suponen casi todos los usuarios de móvil. Por otro lado, depende de que se realice una declaración

responsable de la situación personal de infección, preferiblemente supervisada por un profesional para evitar estrategias de desinformación. Finalmente, es necesario disponer de acceso a tests, no solo para todos los usuarios, sino para poder actualizar la información periódicamente y para que aquellos que sean notificados de haber estado en contacto con un infectado puedan realizar la prueba con prontitud.

No obstante, y siempre bajo un uso respetuoso con la privacidad de los usuarios, se pueden deducir los siguientes beneficios:

- **Beneficios para los interesados:**

  - Las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus serán informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

  Asimismo, se les informará de las medidas que conviene adoptar después, como someterse a autocuarentena o a pruebas, o proporcionar asesoramiento sobre qué hacer en caso de experimentar determinados síntomas.

  - La instalación de la Aplicación en el dispositivo es voluntaria, sin consecuencia negativa alguna para quien decida no descargar o no usar la aplicación.

  - El usuario mantiene el control sus datos personales.

  - El uso de la Aplicación no requiere un seguimiento de la ubicación de los usuarios a título individual; en su lugar, se utilizan datos de proximidad

  - La información recogida se aloja en el equipo terminal del usuario y solo se recoge la información pertinente cuando sea absolutamente necesario.

- **Beneficios para la Administración**

  - Las personas que hayan estado muy cerca de alguien que resulte ser un portador confirmado del virus serán informadas al respecto, a fin de romper las cadenas de transmisión lo antes posible.

  - Tecnología sencilla.

  - La normativa de protección de datos personales contiene una regulación para el uso de casos como lo es el tratamiento que se lleva a cabo con esta Aplicación, que compatibiliza y pondera los intereses y derechos en liza para el bien común.

  - Desempeña un papel importante en la gestión de las medidas de confinamiento durante las posibles situaciones de desescalada.

  - No es necesario que una autoridad almacene información de contacto real.

  - Su repercusión puede reforzarse mediante una estrategia que favorezca la ampliación de las pruebas a las personas que presenten síntomas leves.

  - Puede ser una fuente pertinente de datos para las autoridades sanitarias públicas y facilitar la transmisión de ese tipo de datos a las autoridades epidemiológicas nacionales y al Centro Europeo para la Prevención y el Control de las Enfermedades (ECDC). Esto ayudaría a comprender los patrones de transmisión y, en combinación con los resultados de las pruebas, a estimar el valor predictivo positivo de los síntomas respiratorios en una comunidad dada y proporcionar información sobre el nivel de circulación del virus.

Alternativas al tratamiento y por qué no se han elegido

Como conclusión, cabe señalar que esta Aplicación no puede sustituir, sino meramente apoyar, el rastreo manual de contactos realizado por personal sanitario cualificado, que puede determinar si los contactos estrechos pueden o no dar lugar a una transmisión del virus. Esta labor de rastreo es compleja, principalmente porque exige a los profesionales sanitarios disponer de información rápida y fiable de los contactos de los pacientes, por lo que se puede concluir que el uso de esta Aplicación cumple con los principios de idoneidad ya que el tratamiento evaluado consigue los objetivos propuestos y el juicio de necesidad ya que, actualmente, no existe otra alternativa menos invasiva para la privacidad para conseguir este propósito con la misma eficacia o con una eficacia razonable.

La Aplicación se constituye como una herramienta complementaria de las técnicas tradicionales de rastreo de contactos (en particular, de las entrevistas con personas infectadas), es decir, forma parte de un programa de salud pública de mayor alcance y el objetivo es que sea utilizada exclusivamente hasta el momento en que las técnicas de localización manual de contactos puedan gestionar por sí solas el volumen de nuevas infecciones.

A nuestro criterio, la Aplicación supera el juicio de proporcionalidad.

2.3.8 Medidas para la reducción del riesgo

2.3.8.1 La privacidad desde el diseño

La privacidad desde el diseño implica utilizar un enfoque orientado a la gestión del riesgo y de responsabilidad proactiva para establecer estrategias que incorporen la protección de la privacidad a lo largo de todo el ciclo de vida del objeto (ya sea este un sistema, un producto hardware o software, un servicio o un proceso), en este caso de la Aplicación.

El diseño de los sistemas seguros y confiables se ha centrado en analizar los riesgos y dar respuesta a las amenazas que afectan a los objetivos de la seguridad que están más orientados a la privacidad:

- Confidencialidad, evitando los accesos no autorizados a los sistemas,
- Integridad, protegiéndolos de modificaciones no autorizadas de la información y
- Disponibilidad, garantizando que los datos y los sistemas están disponibles cuando es necesario.

Sin embargo, aunque el acceso y la modificación no autorizada de los datos personales puede llegar a ser un aspecto crítico que amenace la privacidad de los individuos, existen otros factores de riesgo que pueden aparecer durante un procesamiento autorizado de los datos y que deben ser identificados durante la evaluación de riesgos para los derechos y libertades de los sujetos de los datos.

La pérdida de autonomía en la toma de decisiones, la recogida excesiva de datos, la re-identificación, la discriminación y/o estigmatización de las personas, el sesgo en las decisiones automatizadas, la falta de comprensión de los usuarios del alcance y los riesgos de un tratamiento o un perfilado no legitimado, invasivo o incorrecto son ejemplos de riesgos a la privacidad con una clara afectación en los derechos y libertades de las personas que no pueden ser gestionados utilizando un modelo tradicional de riesgos enfocado a la protección exclusiva de los objetivos de seguridad.

Teniendo en cuenta el escenario descrito y los posibles riesgos a la privacidad asociados con el funcionamiento planificado y autorizado de los sistemas que recopilan, usan y divulgan datos personales, es preciso ampliar el marco de análisis para que este cubra tanto los riesgos derivados de su tratamiento no autorizado como aquellos que pueden surgir de un procesamiento planeado y permitido de la información.

Para dar cobertura a estos posibles riesgos han de incluirse en el análisis tres nuevos objetivos de protección, específicos de la privacidad, y cuya garantía se convierte en salvaguarda de los principios de tratamiento establecidos por el RGPD:

- Desvinculación: persigue que el procesamiento de la información se realice de modo que los datos personales de un dominio de tratamiento no puedan vincularse con los datos personales de otro dominio diferente o que el establecimiento de dicha vinculación suponga un esfuerzo desproporcionado. Este objetivo de privacidad minimiza el riesgo de un uso no autorizado de los datos personales y la creación de perfiles mediante la interconexión de información perteneciente a diferentes conjuntos de datos, estableciendo garantías sobre los principios de limitación de la finalidad, la minimización de datos y la limitación del plazo de conservación.

- Transparencia: busca clarificar el tratamiento de los datos de modo que la recogida, el procesamiento y el uso de la información pueda ser comprendido y reproducido por cualquiera de las partes implicadas y en cualquier momento del tratamiento. Este objetivo de la privacidad pretende que el contexto del tratamiento quede perfectamente delimitado y que la información sobre las finalidades y las condiciones legales, técnicas y organizativas aplicables esté disponible antes, durante y después del tratamiento a todas las partes implicadas, tanto para el responsable como para el sujeto cuyos datos son tratados, minimizando así los riesgos que pueden afectar a los principios de lealtad y transparencia.

• Control: garantiza la posibilidad de que las partes involucradas en el tratamiento de los datos personales y, principalmente, los sujetos cuyos datos son tratados, pueden intervenir en el tratamiento cuando sea necesario para aplicar medidas correctivas al procesamiento de la información. Este objetivo está íntimamente relacionado con la definición e implementación de procedimientos para el ejercicio de derechos en materia de protección de datos, la presentación de reclamaciones o la revocación de los consentimientos prestados por parte de los interesados, así como mecanismos para garantizar, por parte del responsable, la evaluación del cumplimiento y la efectividad de las obligaciones que le son fijadas por la normativa, lo que contribuye a respetar los principios de exactitud y responsabilidad proactiva marcados por el RGPD.

Vistos de forma global y conjunta, los objetivos de protección son complementarios entre sí y en ocasiones se solapan, por lo que, para cada evaluación de impacto sobre la protección de datos (EIPD) que se realice sobre los tratamientos de datos a acometer, habrá que valorar la posible preponderancia de un objetivo sobre otro y buscar un equilibrio en las medidas y salvaguardas adoptadas para su garantía.

La implementación eficaz y eficiente de los principios de privacidad han sido tenidos en cuenta desde la fase inicial de concepción, diseño y desarrollo de la Aplicación como una parte más del conjunto de especificaciones, funcionales y no funcionales, utilizando un enfoque metodológico orientado a la gestión del riesgo y de responsabilidad proactiva que permita fijar los requisitos de privacidad mediante prácticas, procedimientos y herramientas.

Con relación a las aplicaciones de rastreo de contactos la Unión Europea ha publicado una serie de recomendaciones: las autoridades sanitarias deberán aprobar las aplicaciones y ser responsables del cumplimiento de la normativa europea de protección de datos incluyendo a las autoridades nacionales de protección de datos; los usuarios deben tener control total sobre sus datos; la instalación de la app debe ser voluntaria; no se podrán rastrear los movimientos de las personas; los datos deben almacenarse de forma cifrada únicamente en los móviles; las apps deben ser interoperables entre países de la UE y deberían desactivarse en cuanto no sean necesarias.

La mayoría de las soluciones caben en dos categorías, centralizadas o descentralizadas, y se diferencian en los grados de protección de la privacidad para la ciudadanía. El punto común es que todas se basan en el uso de Bluetooth para detectar a personas a nuestro alrededor con las que hemos coincidido.

La opción centralizada consiste en el envío sistemático de información de interacciones de riesgo con personas a un servidor central. En este caso, se intenta mantener el anonimato dando al móvil un código (o pseudo-identificador) que permite que el servidor central notifique alguna interacción con un positivo de COVID-19 pero no permite identificar a la persona.

La opción descentralizada, por la que se ha optado en el desarrollo de la Aplicación es más afín a la “privacidad desde el diseño” y consiste en mantener los datos exclusivamente en el móvil de una persona (descentralizada) y evitar el uso de identificadores que puedan revelar la identidad de la persona pero que permitan que el sistema funcione.

En este caso, cada terminal genera una serie de identificadores efímeros (cadenas de caracteres aleatorias) que emite a través de Bluetooth. Estas cadenas cambian cada poco tiempo de manera que otros terminales pueden guardarlas y estimar cuánto tiempo han estado cerca de una persona sin saber quién es esta persona.

En este caso, tanto los identificadores efímeros producidos como detectados se almacenan únicamente en el teléfono. Ante un caso positivo los identificadores efímeros generados desde un terminal se añadirían a una base de datos central que los teléfonos de todos los ciudadanos descargarían periódicamente para comprobar que los identificadores que han ido almacenando coinciden con los de alguna persona que haya dado positivo.

De esta forma no se puede revelar la identidad de ninguna persona ni el lugar de la interacción.

Por tanto, en el diseño de esta Aplicación se ha tenido en cuenta la “privacidad desde el diseño” porque la privacidad se garantiza a nivel de diseño y código, y no se implementa en base a confianza a terceras partes.

Analizando el funcional de la Aplicación, se puede comprobar lo siguiente:

Una vez que una persona tiene la Aplicación en su teléfono, esta genera una clave anónima que va refrescándose y cambiando cada cierto tiempo («identidades efímeras»). El dispositivo emite estas identidades efímeras por Bluetooth hacia el resto de los dispositivos que se encuentren cerca y viceversa. De forma que los identificadores se van quedando almacenados en el propio teléfono. Así, un móvil genera una

lista de todos los identificadores con los que se ha encontrado. Si una persona, a través de un test, da positivo en covid-19, se activaría el sistema, de forma que su aplicación, con permiso del usuario, enviaría el TEK positivo al servidor central. El servidor central envía este a todos los móviles y son estos últimos los que regeneran los RPI asociados y los comparan con los almacenados internamente. El servidor no tiene ninguna información relevante, solo los números de las personas infectadas. Es un canal de comunicación. Por eso es totalmente anónimo.

Para que el concepto de privacidad por diseño sea plenamente eficaz en esta Aplicación es esencial que exista una seguridad de que se pueda impedir que haya terceros que puedan usar la información que obtiene la aplicación. Es la forma de no tener que depositar la confianza en que los terceros o empresas que participen en el proceso vayan a hacer un uso ético de la información que manejan o que puedan proteger adecuadamente esos datos.

En resumen se puede afirmar que en esta Aplicación se ha prestado especial atención al principio de minimización de datos y a la protección de datos desde el diseño y por defecto:

- las aplicaciones de rastreo de contactos no requieren un seguimiento de la ubicación de los usuarios a título individual; en su lugar, deben utilizarse datos de proximidad;
- la información recogida debe alojarse en el equipo terminal del usuario y solo debe recogerse la información pertinente cuando sea absolutamente necesario.
- se trata de aplicaciones que pueden funcionar sin la identificación directa de personas.

Es importante, no obstante, tener en cuenta que como se trata de aplicaciones que pueden funcionar sin la identificación directa de personas, conviene establecer medidas adecuadas para prevenir la re-identificación. Los requisitos funcionales recogidos por la Aplicación en cumplimiento de las medidas de protección de datos desde el diseño y por defecto son las siguientes:

- La Aplicación no recoge información que no tenga relación con el objeto específico o no sea necesaria — por ejemplo, estado civil, identificadores de las comunicaciones, elementos del directorio del equipo, mensajes, registros de llamadas, datos de localización, identificadores de dispositivos, etc.
- Los datos difundidos por las aplicaciones solo incluyen algunos identificadores únicos y seudónimos, generados por la Aplicación y específicos de esta. Esos identificadores renuevan periódicamente, con una frecuencia compatible con el propósito de contener la propagación del virus y suficiente para limitar el riesgo de identificación y de rastreo físico de personas.
- Aunque el modelo es descentralizado, siempre va a ser necesario un servidor central, de la autoridad sanitaria. Este servidor de rastreo de contactos debe limitarse a recoger las claves de los TEK positivos. El servidor central envía este a todos los móviles y son estos últimos los que regeneran los RPI asociados y los comparan con los almacenados internamente.
- Se aplicarán técnicas criptográficas avanzadas, como es el cifrado asimétrico, para garantizar la seguridad de los datos almacenados en los servidores y aplicaciones y los intercambios entre las aplicaciones y el servidor remoto. También se procederá a la autenticación mutua entre la Aplicación y el servidor.
- La notificación de los usuarios infectados de SARS-CoV-2 en la Aplicación se someterá a una autorización adecuada mediante un código de un solo uso unido a una identidad seudónima de la persona infectada y vinculado con un laboratorio de pruebas de detección o con un profesional de atención sanitaria. Si no se puede obtener confirmación de forma segura, no tendrá lugar ningún tratamiento de datos que presuponga la validez del estado del usuario.
- El responsable del tratamiento, en colaboración con las autoridades públicas, tiene que facilitar información clara y explícita sobre el enlace que permita descargar la Aplicación oficial nacional de rastreo de contactos, con el fin de mitigar el riesgo de que se utilicen aplicaciones de terceros.
- En virtud de los principios de integridad y confidencialidad, teniendo en cuenta que los datos de salud merecen una protección más elevada, se aplicarán medidas de carácter técnico y organizativo actualizadas adecuadas que garanticen un nivel de seguridad suficiente. Tales

medidas consisten en la seudonimización, el cifrado y la celebración de acuerdos de confidencialidad, así como en una distribución estricta de los roles de acceso y el establecimiento de restricciones y registros de acceso. Asimismo, hay que tener en cuenta las disposiciones nacionales que pueden establecer requisitos técnicos concretos u otras garantías, tales como la observancia de las normas de secreto profesional.

3 EVALUACIÓN DE RIESGOS Y SALVAGUARDAS

La evaluación de riesgos realizada para el servicio "Radar COVID" se encuentra recogida en el "Análisis de Riesgos Servicio Radar Covid", generado con la herramienta "PILAR" (en adelante, el Informe de AARR) mediante el que se ha llevado a cabo la evaluación de riesgos y salvaguardas para el tratamiento "Radar COVID" y toda la infraestructura que se ha implementado para este servicio.

Dicho Análisis de Riesgos se ha llevado a cabo de acuerdo con las siguientes actividades:

3.1 Caracterización de activos

En el Informe de AARR se recoge una identificación y valoración de los activos que forman parte del alcance del Análisis de Riesgos.

La valoración se realiza de acuerdo con las dimensiones de seguridad: Autenticidad, Confidencialidad, Integridad, Disponibilidad y Auditabilidad o Trazabilidad, referidas en el citado informe como valoración ACIDA.

La valoración se ha determinado teniendo en cuenta la Guía CCN-STIC 803 ENS "Valoración de los sistemas".

También se recoge en el Anexo I de Informe de AARR: Inventario de Activos, donde se incorpora la información relativa al RGPD, información que se recoge, asimismo, de manera detallada a lo largo del presente Informe (roles, necesidad, ciclo de vida y necesidad y proporcionalidad).

Los valores que puede tomar cada una de las dimensiones son: Sin Valorar (No Adscrito), Bajo, Medio y Alto. Los criterios para determinar la valoración de las dimensiones de seguridad se recogen en el Anexo II del Informe de AARR: Criterios de Valoración de Sistemas de Información.

3.2 Caracterización de amenazas

Una vez realizada la caracterización de los activos, a continuación, se ha procedido a **identificar las amenazas** sobre cada uno de los Activos de Información, estimando la frecuencia de ocurrencia y el daño (degradación) que causarían.

Los valores de degradación de activos y frecuencia de amenazas utilizados son los que proporciona la herramienta PILAR, no obstante, se han modificado los valores de Frecuencia de algunas amenazas para adaptarlos a las características particulares del entorno del ***Servicio Radar Covid***. Dichas modificaciones se recogen en el Anexo IV del Informe de AARR: Información Modificada de Amenazas.

El detalle de todas las amenazas asociadas a los distintos activos junto a la frecuencia y degradación en cada una de las dimensiones se puede consultar en el archivo ***00 Pilar - covid 2 - ENS - GDPR v2.0.mgr***.

Con toda esta información se determina el **Riesgo Potencial**, como la medida del daño probable sobre un sistema.

3.3 Principales amenazas identificadas

A continuación, se presenta el listado de las principales amenazas, que según el Informe de AARR, pueden afectar al tratamiento, pues son las que tienen un mayor nivel de riesgo, y son las que convendría tener en cuenta para disminuir el riesgo actual a niveles más bajos. Los niveles representados son los siguientes:

[001] Servicio Radar Covid19	5,9	6,3	2,4	5,1	5	6,3
[A.11] Acceso no autorizado		6,3		5,1		6,3
[A.5] Suplantación de la identidad	5,9	5,4		4,2		5,9
[A.6] Abuso de privilegios de acceso		5,4	2,4	4,2		5,4
[PR.g9] 9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma					5	5
[PR.g8] 8. No tramitar o dificultar el ejercicio de los derechos de los interesados					5	5
[PR.g1] 1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fác					4,1	4,1

En cuanto a las amenazas correspondientes a los Datos de Carácter Personal se han utilizado las amenazas estándar registradas en la Herramienta PILAR, cuyos valores de frecuencia de algunas amenazas han sido modificados para adaptarlos a las características particulares del entorno del ***Servicio Radar Covid***. asociando los valores de Frecuencia y Degradación recogidos en la tabla que sigue a continuación:

Amenazas PILAR [Datos Personales]		Frecuencia	Degradación
[PR.g1]	1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender	0,1	MA
[PR.g2]	2. Tratar datos inadecuados y excesivos para la finalidad del tratamiento	0,01	MA
[PR.g3]	3. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos	0,01	MA
[PR.g4]	4. Tratar los datos personales con una finalidad distinta para la cual fueron recabados	0,01	MA
[PR.g5]	5. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización	0,01	MA
[PR.g6]	6. Almacenar los datos por periodos superionres a los necesarios para la finalidad del tratamiento y a la legislación vigente	0,01	MA
[PR.g7]	7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado	0,01	MA
[PR.g8]	8. No tramitar o dificultar el ejercicio de los derechos de los interesados	1	MA
[PR.g9]	9. Resolución indebida del ejercicio de derechos de los interesados en tiempo, formato y forma	1	MA
[PR.g10]	10. Seleccionar o mantener una relación con el encargado de tratamiento sin disponer de las garantías adecuadas	0,1	M
[PR.g11]	11. Carecer de mecanismos de supervisión y control sobre las medidas que regulan la relación con un encargado de tratamiento	0,1	M
[PR.g12]	12. No registrar la creación, modificación o cancelación de las actividades de tratamiento efectuadas bajo su responsabilidad	0,01	M
[PR.g13]	13. No llevar a cabo por parte del responsable del tratamiento una evaluación de impacto adecuada en los supuestos detallados por la normativa aplicable	0,01	M
[PR.g23]	23. Disociación deficiente o reversible que permita re-identificación de datos	0,1	M
[PR.g24]	24. Información no actualizada o incorrecta (pe. registros duplicados con informaciones contradictorias o con campos de datos incorrectos)	0,01	M
[PR.g32]	32. Deficiencias en los protocolos de almacenamiento de los datos personales en formato físico	0,1	M

Una vez determinado que una amenaza puede perjudicar a un activo, se ha **valorado** mediante la Herramienta PILAR su impacto en el activo, en dos sentidos:

- *Degradación*: Estima el daño causado por una amenaza en el supuesto de que se materializara.
- *Frecuencia*: Es una estimación de cada cuánto tiempo se materializa la amenaza.

Los valores que se han utilizado de degradación y frecuencia están ampliamente reconocidos y son los siguientes:

Degradación	Descripción
100% Total (T)	El activo queda totalmente inutilizado, causando un daño excepcional sobre su misión para la Organización
90% Muy alta (MA)	El activo ha sufrido importantes daños, que muy probablemente tengan serias repercusiones sobre su misión en la Organización.
50% Alta (A)	Aunque la degradación ha sido importante, el activo (o un respaldo suyo) puede seguir funcionando.
10% Media (M)	Se producen daños en el activo que pueden causar pérdidas menores o mermas en la seguridad sobre ciertos aspectos.
1% Baja (B)	La degradación sería causa de inconveniencias mínimas sobre la Organización.

Frecuencia	Descripción
100	Muy frecuente. A diario
10	Frecuente. Mensualmente
1	Normal. Una vez al año.
0,1	Poco frecuente. Cada varios años.
0,01	Muy rara

3.4 Valor del Riesgo Potencial

Una vez identificadas las amenazas a las que están expuestos los activos se caracterizan en el Informe de AARR por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación).

De este modo se lleva a cabo una estimación del riesgo potencial o intrínseco sobre cada uno de los activos.

Los valores de riesgo utilizados por la Herramienta PILAR se pueden clasificar en una escala del 0 al 10, como muestra la tabla siguiente:

Valor	Interpretación
{0-1}	Riesgo despreciable.
{1-2}	Riesgo bajo.
{2-3}	Riesgo medio.
{3-4}	Riesgo alto.
{4-5}	Riesgo muy alto.
{5-6}	Riesgo crítico.
{6-7}	Riesgo muy crítico
{7-10}	Riesgo extremadamente crítico

Tabla 2. Escala de valores de riesgo

El detalle de los riesgos potenciales asociados a los activos de información son los siguientes:

ACTIVOS	RIESGO POTENCIAL
[001] Servicio Radar Covid19	6,3
[HW-0001] Teléfono Móvil	2,7
[COM-0001] Redes de Comunicaciones	5,3
[SW-0001] App Radar Covid19	5,1
[P-0002] Administradores / Operadores	4,8
[SS-0001] Desarrollo y Mantenimiento de la App	4,2
[P-0003] Desarrolladores	4,2
[P-0001] Ciudadanos	3,7
[SP-0001] Soportes	5,7
[L-0001] Instalaciones AWS	5,1
[HW-0002] Equipos AWS	5,1
[SE-0002] Repositorio Descargas (APPLE STORE)	4,2
[SS-0002] Servicio Cloud	4,2
[SE-0001] Repositorio Descargas (ANDROID STORE)	4,2

Tabla 3. Riesgo potencial

A continuación, se muestra la relación entre el número de activos de información y su nivel de riesgo atendiendo a los valores de riesgo potencial de la tabla anterior:

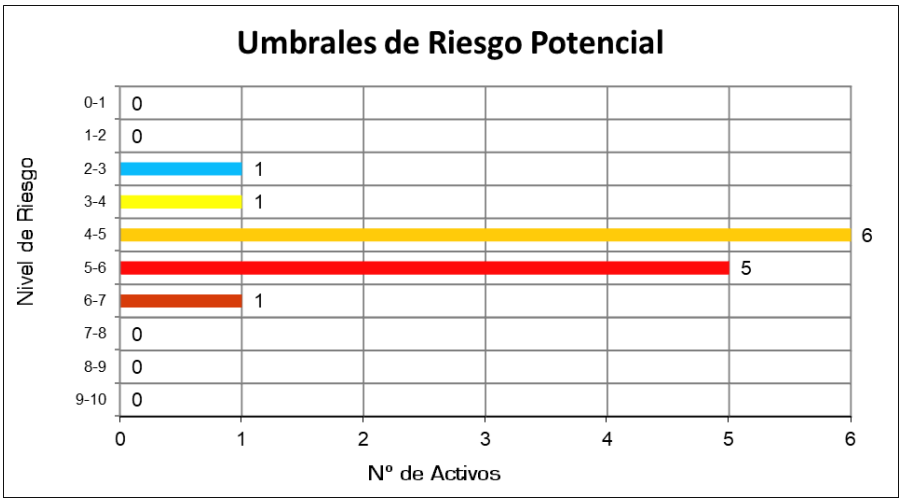

Ilustración 2. Número de activos por nivel de riesgo potencial

3.3 Tratamiento de los Riesgos-Evaluación de Salvaguardas

Las salvaguardas son los procedimientos o mecanismos tecnológicos que reducen el riesgo.

La caracterización de las salvaguardas se ha realizado mediante la cumplimentación de un Cuestionario Técnico basado en el Anexo II del Informe del AARR: Medidas de Seguridad, del Esquema Nacional de Seguridad (RD 951/2015), que constituyen las medidas implementadas por la Herramienta PILAR. Así mismo, para la definición de los controles se ha tenido en cuenta Guía CCN-STIC-808: Verificación del Cumplimiento del ENS.

Además, se ha incorporado el catálogo de salvaguardas del RGPD implementado por PILAR. Se han catalogado los diferentes controles aplicables del RGPD valorando su nivel de madurez para este tratamiento lo que, debido al elevado nivel de madurez de la mayor parte de estos controles hacen que los riesgos sean casi inexistentes y las amenazas correspondientes a los Datos de Carácter Personal detectadas por la herramienta queden mitigadas.

Las salvaguardas se caracterizan por su eficacia frente al riesgo que pretenden mitigar. Para la **valoración** de la eficacia de las medidas de seguridad se ha utilizado el **Modelo de Madurez de la Capacidad** (CMM - Capability Maturity Model), cuyos valores implementados por la Herramienta PILAR son los siguientes:

Nivel de Madurez	Descripción
L0	*Inexistente (0 %)* Esta medida no existe o no está siendo aplicada en este momento.
L1	*Inicial / Ad Hoc (10 %)* La organización no proporciona un entorno estable. El proceso existe, pero no se gestiona

Nivel de Madurez	Descripción
	Estado inicial donde el éxito de las actividades de los procesos se basa, la mayoría de las veces, en el esfuerzo personal. El éxito o fracaso del proceso depende de la competencia y buena voluntad de las personas y es difícil prever la reacción ante una situación de emergencia. Los procedimientos son inexistentes o localizados en áreas concretas. No existen plantillas definidas a nivel corporativo.
L2	*Reproducible pero Intuitivo (50%) o Parcialmente Realizado* La eficacia del proceso depende del grado de conocimiento de cada individuo. Los procesos similares se llevan en forma similar por diferentes personas. Es impredecible el resultado si se dan circunstancias nuevas. Se normalizan las buenas prácticas en base a la experiencia. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.
L3	*Proceso Definido (90 %) o En Funcionamiento* Los procesos están implantados, documentados y comunicados mediante entrenamiento. La Organización entera participa en el proceso y existe una coordinación entre departamentos.
L4	*Gestionado y Medible (95 %) o Monitorizado* Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos. Se dispone de la tecnología adecuada para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia. La Dirección es capaz de establecer objetivos cualitativos a alcanzar y dispone de medios para valorar si se han alcanzado los objetivos y en qué medida.
L5	*Optimizado (100 %)* Se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras. Se pueden establecer objetivos cuantitativos de mejora. Basados en los criterios cuantitativos se pueden determinar las desviaciones más comunes y se pueden optimizar los procesos.

La información recopilada sobre el grado de madurez de los controles se encuentra recogida en el Anexo III el Informe del AARR: Caracterización de las Salvaguardas.

La caracterización de las salvaguardas se ha realizado mediante reuniones con los responsables técnicos, responsables del desarrollo, puesta en marcha e implantación de la **Aplicación,** quienes conocen su infraestructura y que, por tanto, pueden conocer el grado de implantación de cada una de las medidas de seguridad**.** En estas reuniones se ha recopilado la información para conocer el estado de las medidas de seguridad que se encuentran en el *Anexo II del Informe de AARR: Medidas de Seguridad,* del Esquema Nacional de seguridad (RD 951/2015) para, posteriormente, incorporar dicho estado en el catálogo de PILAR.

De la misma manera, se ha identificado el grado de madurez de cada uno de los artículos del RGPD que deben ser tenidos en consideración.

La información recopilada sobre el grado de madurez de las medidas de seguridad del ENS y de los artículos del RGPD se encuentra recogida en el apartado *Anexo III del Informe de AARR: Caracterización de las Salvaguardas*.

3.4 Valor de riesgo actual o residual

El valor de riesgo actual o residual se muestra en el Informe del AARR como el resultado de caracterizar las amenazas a las que están expuestos los activos y determinar la eficacia de las salvaguardas actualmente desplegadas.

El detalle de los riesgos residuales asociados a los activos de información son los siguientes:

ACTIVOS	RIESGO RESIDUAL
[001] Servicio Radar Covid19	2,6
[HW-0001] Teléfono Móvil	0,47
[COM-0001] Redes de Comunicaciones	0,97
[SW-0001] App Radar Covid19	0,91
[P-0002] Administradores / Operadores	0,81
[P-0003] Desarrolladores	0,69
[SS-0001] Desarrollo y Mantenimiento de la App	0,83
[P-0001] Ciudadanos	0,58
[SP-0001] Soportes	1
[HW-0002] Equipos AWS	0,96
[L-0001] Instalaciones AWS	0,95
[SE-0002] Repositorio Descargas (APPLE STORE)	0,83
[SS-0002] Servicio Cloud	0,83
[SE-0001] Repositorio Descargas (ANDROID STORE)	0,83

Tabla 4. Riesgo residual

A continuación, tal y como se expone en el Informe de AARR realizado, se muestra la relación entre el número de activos de información y su nivel de riesgo atendiendo a los valores de riesgo residual de la tabla anterior:

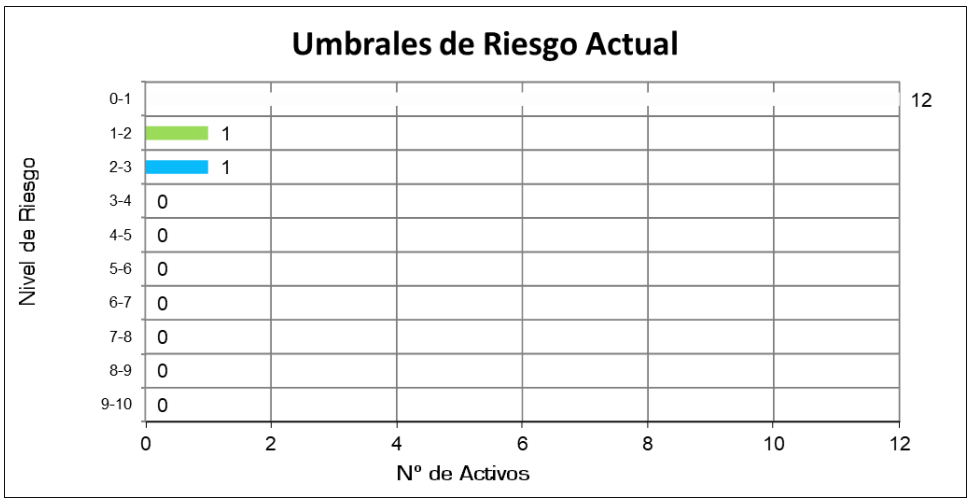

Ilustración 3. Número de activos por nivel de riesgo residual

Como ya se ha expuesto anteriormente los riesgos o amenazas que podrían afectar en mayor medida al debido cumplimiento de la legislación en materia de privacidad y por tanto a los datos personales de los usuarios serían:

. - Que no se proporcione suficiente información y que esta información no sea clara y concisa en cuanto a las finalidades o propósito del tratamiento, es decir, el principio de transparencia en la información a los interesados.

Este riesgo se encuentra mitigado debido a la correcta implementación de la información que se facilita a los usuarios en la política de privacidad a las que deben acceder y aceptar antes de usar la Aplicación.

. - Que los interesados no puedan ejercitar sus derechos, que sean debidamente informados de ello y sean atendidos en tiempo y forma.

En cuanto a esta amenaza también se encuentra en parte mitigado en cuanto a que en la Política de Privacidad de acceso a la Aplicación se informa a los usuarios de la posibilidad de ejercitar sus derechos ante el Responsable de los datos.

En todo caso, sería conveniente, tal y como se pone de manifiesto en el siguiente apartado, llevar a cabo una serie de acciones para mitigar de manera segura este riesgo.

4 PROPUESTA DE ACCIONES DERIVADAS DE LA EIPD

4.1 Plan de Acción o de tratamiento de riesgos

Para realizar el Plan de Acción o tratamiento de Riesgos se tienen que tener en cuenta aquellos riesgos que la organización no está dispuesta a asumir. Normalmente este valor se suele fijar en un nivel ALTO, que en la escala de PILAR es a partir de un valor {3}. En el caso del Servicio Radar COVID, como puede comprobarse en el Informe de AARR, todos los riesgos han salido por debajo de 3, siendo el riesgo residual identificado más alto con un riesgo de nivel MEDIO cuyo valor es {2,6}.

4.1.1 Plan de acción

Para el Servicio Radar COVID se propone en el Informe de AARR, realizar una serie de acciones necesarias para minimizar el riesgo residual de manera que no haya ningún activo con riesgo de nivel MEDIO. Para ello se han seleccionado aquellos riesgos que se encuentran por encima del valor {2} y, sobre ellos, se han identificado las salvaguardas que se encontraban por debajo del valor recomendado por PILAR para el Esquema Nacional de Seguridad para subirlas al valor recomendado.

4.1.2 Riesgo Objetivo

La implementación de las acciones de mejora propuestas en el Informe del AARR, permitirían alcanzar un valor de riesgo objetivo suficiente para realizar el tratamiento, sin perjuicio de emprender acciones adicionales que sirvan para reducir aún más el nivel de riesgo residual o actual.

Con estas premisas, el nivel de madurez debería tender a cubrir las especificaciones del Esquema Nacional de Seguridad en los plazos que se estimen adecuados.

Una vez implantadas las salvaguardas propuestas, el detalle de los riesgos objetivos asociados a los activos de información serían los siguientes:

ACTIVOS DE INFORMACIÓN	RIESGO OBJETIVO
[001] Servicio Radar Covid19	1,8
[HW-0001] Teléfono Móvil	0,47
[COM-0001] Redes de Comunicaciones	0,97
[SW-0001] App Radar Covid19	0,91
[P-0002] Administradores / Operadores	0,81
[P-0003] Desarrolladores	0,69
[SS-0001] Desarrollo y Mantenimiento de la App	0,83
[P-0001] Ciudadanos	0,58
[SP-0001] Soportes	1
[HW-0002] Equipos AWS	0,96
[L-0001] Instalaciones AWS	0,95
[SE-0002] Repositorio Descargas (APPLE STORE)	0,83
[SS-0002] Servicio Cloud	0,83
[SE-0001] Repositorio Descargas (ANDROID STOR	0,83

Tabla 5. Riesgo objetivo

A continuación, se muestra la relación entre el número de activos de información y su nivel de riesgo atendiendo a los valores de riesgo objetivo de la tabla anterior:

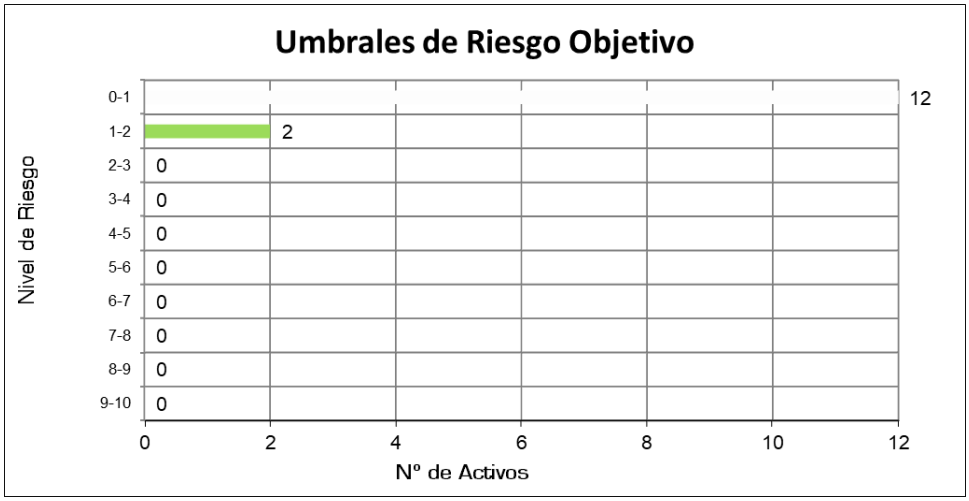

Ilustración 4. Número de activos por nivel de riesgo objetivo

Como puede observarse, una vez que se realicen las acciones propuestas en el Informe de AARR, no hay ningún activo con riesgo medio. En la gráfica se puede observar que hay 12 activos con riesgo despreciable y 2 con riesgo bajo.

En cuanto al posible riesgo derivado de que que los interesados no puedan ejercitar sus derechos, que sean debidamente informados de ello y sean atendidos en tiempo y forma, se recomienda que se pueda garantizar el acceso a los datos en todo momento a través de la Aplicación, que estén debidamente informados sobre dónde deben ejercitarlos y que existan procedimientos internos para poder atenderlos debidamente.

5 CONCLUSIONES

En el presente Informe se documentan los resultados obtenidos durante las distintas fases de la Evaluación de Impacto relativa a la Protección de Datos del tratamiento "Radar COVID", según lo exigido en el artículo 35 del RGPD.

En primer lugar, se ha realizado una caracterización o contextualización del tratamiento. Para ello se ha descrito la necesidad de realizar la EIPD sobre el mencionado tratamiento, así como todos aquellos aspectos que permiten conocer en detalle todo el ciclo de vida y el flujo de datos personales a través del mismo, incluyendo todos los actores y elementos intervinientes durante las distintas fases del tratamiento.

Esto nos ha permitido obtener una visión en detalle que facilita la identificación de las amenazas y los riesgos a los que están expuestos los datos personales asociados al mismo.

Posteriormente, se ha realizado un análisis de la necesidad y proporcionalidad del tratamiento. A tal objeto, en el apartado 2.3.6 se ha identificado la existencia de varias bases jurídicas claras y suficientes, que habilitan y amparan la licitud del tratamiento en la prestación del consentimiento de los interesados y en la concurrencia de disposiciones legales específicas.

Asimismo, se ha verificado el cumplimiento de los principios de limitación de la finalidad, minimización de los datos tratados y limitación del plazo de conservación. Por estos motivos, se entiende suficientemente justificada la legitimidad y la proporcionalidad del tratamiento.

En segundo lugar, se han valorado las amenazas a las que está expuesto el tratamiento y los controles y salvaguardas implementados para reducir su exposición a las mismas utilizando la Aplicación.

Teniendo en cuenta la escala de valoración del nivel de riesgo 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]**.

Sin embargo, atendiendo a los niveles mínimos de madurez requeridos por el Esquema Nacional de Seguridad y tomando como métrica para el nivel de riesgo el mayor valor de riesgo identificado en un activo, igual que para el riesgo residual, el objetivo que se propone alcanzar en el proceso de mitigación de riesgos quedaría establecido en un **Nivel de Riesgo Objetivo = [1,8]**.

ACTIVOS DE INFORMACIÓN	RIESGO RESIDUAL	RIESGO OBJETIVO
[001] Servicio Radar Covid19	2,6	1,8
[HW-0001] Teléfono Móvil	0,47	0,47
[COM-0001] Redes de Comunicaciones	0,97	0,97
[SW-0001] App Radar Covid19	0,91	0,91
[P-0002] Administradores / Operadores	0,81	0,81
[P-0003] Desarrolladores	0,69	0,69
[SS-0001] Desarrollo y Mantenimiento de la App	0,83	0,83
[P-0001] Ciudadanos	0,58	0,58
[SP-0001] Soportes	1	1
[HW-0002] Equipos AWS	0,96	0,96
[L-0001] Instalaciones AWS	0,95	0,95
[SE-0002] Repositorio Descargas (APPLE STORE)	0,83	0,83
[SS-0002] Servicio Cloud	0,83	0,83
[SE-0001] Repositorio Descargas (ANDROID STORE)	0,83	0,83

Tabla 6. Evolución de los riesgos

Para ello se han propuesto una serie de acciones y recomendaciones en el Informe de AARR cuya implantación supondría que ninguno de los activos alcanzaría un riesgo medio, sino que todos se podrían calificar de riesgo bajo e incluso muchos de ellos de riesgo despreciable.

En cuanto a los riesgos referidos a la protección de datos personales de los usuarios, el riesgo detectado es mínimo debido a la madurez de los controles RGPD implementados para este tratamiento, plasmando en el Análisis de Riesgos las posibles amenazas y sus planes de acción para su correcta mitigación.

Por tanto, entendemos siempre sometido a mejor criterio por parte del Responsable del Tratamiento y/o al Delegado de Protección de Datos de la Dirección General de Salud Pública del Ministerio de Sanidad que, teniendo en cuenta todo lo anterior, no es necesario realizar la consulta previa del artículo 36 del RGPD a la Agencia Española de Protección de Datos (AEPD), siendo posible su tratamiento, siempre y cuando se observen las medidas de seguridad y planes de acción descritos en el Informe de Análisis de Riesgos, así como los principios y obligaciones establecidas en la norma.

Asimismo, hay que poner de manifiesto que se han mantenido diversos contactos e interacciones a nivel informativo con la AEPD durante el desarrollo de la Aplicación, y se ha trabajado en dicho desarrollo teniendo en cuenta, en todo momento, sus indicaciones y la normativa aplicable con el fin de garantizar los derechos y libertades de las personas y la seguridad de los datos.

En Madrid, noviembre de 2020.

6 ANEXO I. DEFINICIONES, ACRÓNIMOS Y EXPRESIONES

Definiciones

Las siguientes definiciones proceden del artículo 4 del Reglamento (UE) 2016/679:

- «**datos personales**»: toda información sobre una persona física identificada o identificable («el interesado»); se considerará persona física identificable toda persona cuya identidad pueda determinarse, directa o indirectamente, en particular mediante un identificador, como por ejemplo un nombre, un número de identificación, datos de localización, un identificador en línea o uno o varios elementos propios de la identidad física, fisiológica, genética, psíquica, económica, cultural o social de dicha persona.
- «**tratamiento**»: cualquier operación o conjunto de operaciones realizadas sobre datos personales o conjuntos de datos personales, ya sea por procedimientos automatizados o no, como la recogida, registro, organización, estructuración, conservación, adaptación o modificación, extracción, consulta, utilización, comunicación por transmisión, difusión o cualquier otra forma de habilitación de acceso, cotejo o interconexión, limitación, supresión o destrucción.
- «**limitación del tratamiento**»: el marcado de los datos de carácter personal conservados con el fin de limitar su tratamiento en el futuro.
- «**elaboración de perfiles**»: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales para evaluar determinados aspectos personales de una persona física, en particular para analizar o predecir aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad, comportamiento, ubicación o movimientos de dicha persona física.
- «**seudonimización**»: el tratamiento de datos personales de manera tal que ya no puedan atribuirse a un interesado sin utilizar información adicional, siempre que dicha información adicional figure por separado y esté sujeta a medidas técnicas y organizativas destinadas a garantizar que los datos personales no se atribuyan a una persona física identificada o identificable.
- «**responsable del tratamiento**» o «**responsable**»: la persona física o jurídica, autoridad pública, servicio u otro organismo que, solo o junto con otros, determine los fines y medios del tratamiento; si el Derecho de la Unión o de los Estados miembros determina los fines y medios del tratamiento, el responsable del tratamiento o los criterios específicos para su nombramiento podrá establecerlos el Derecho de la Unión o de los Estados miembros.
- «**encargado del tratamiento**» o «**encargado**»: la persona física o jurídica, autoridad pública, servicio u otro organismo que trate datos personales por cuenta del responsable del tratamiento.
- «**destinatario**»: la persona física o jurídica, autoridad pública, servicio u otro organismo al que se comuniquen datos personales, se trate o no de un tercero. No obstante, no se considerarán destinatarios las autoridades públicas que puedan recibir datos personales en el marco de una investigación concreta de conformidad con el Derecho de la Unión o de los Estados miembros; el tratamiento de tales datos por dichas autoridades públicas será conforme con las normas en materia de protección de datos aplicables a los fines del tratamiento.
- «**tercero**»: persona física o jurídica, autoridad pública, servicio u organismo distinto del interesado, del responsable del tratamiento, del encargado del tratamiento y de las personas autorizadas para tratar los datos personales bajo la autoridad directa del responsable o del encargado.

- «**consentimiento del interesado**»: toda manifestación de voluntad libre, específica, informada e inequívoca por la que el interesado acepta, ya sea mediante una declaración o una clara acción afirmativa, el tratamiento de datos personales que le conciernen.
- «**violación de la seguridad de los datos personales**»: toda violación de la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de datos personales transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizados a dichos datos.
- «**datos genéticos**»: datos personales relativos a las características genéticas heredadas o adquiridas de una persona física que proporcionen una información única sobre la fisiología o la salud de esa persona, obtenidos en particular del análisis de una muestra biológica de tal persona.
- «**datos biométricos**»: datos personales obtenidos a partir de un tratamiento técnico específico, relativos a las características físicas, fisiológicas o conductuales de una persona física que permitan o confirmen la identificación única de dicha persona, como imágenes faciales o datos dactiloscópicos.
- «**datos relativos a la salud**»: datos personales relativos a la salud física o mental de una persona física, incluida la prestación de servicios de atención sanitaria, que revelen información sobre su estado de salud.
- «**representante**»: persona física o jurídica establecida en la Unión que, habiendo sido designada por escrito por el responsable o el encargado del tratamiento con arreglo al artículo 27, represente al responsable o al encargado en lo que respecta a sus respectivas obligaciones en virtud del presente Reglamento.

Acrónimos

- **AEPD**: Agencia Española de Protección de Datos.
- **SEDIA:** Secretaría de Estado de Digitalización e Inteligencia Artificial
- **EIDP** (Evaluación del Impacto en la Privacidad de los Datos)
- **PILAR:** Procedimiento. Informático y Lógico de Análisis de Riesgos
- **GDPR**: 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).


GOBIERNO
DE ESPAÑA
MINISTERIO
DE ASUNTOS ECONÓMICOS
Y TRANSFORMACIÓN DIGITAL
SECRETARÍA DE ESTADO
DE DIGITALIZACIÓN
E INTELIGENCIA ARTIFICIAL