

Radar COVID

Análisis de riesgos

Utilizando las últimas tecnologías para contener la pandemia Covid-19

Versión 3.0

4 de noviembre de 2020

Índice

1. Introducción	3
1.1 Objetivos	4
1.2 Alcance	4
1.3 Estructura del documento	4
1.4 Referencias Documentales	5
2. Metodología de Análisis de Riesgos	6
2.1 Caracterización de Activos	7
2.2 Caracterización de Amenazas	8
2.3 Evaluación de Salvaguardas	10
2.4 Estado del Riesgo	13
2.4.1 Riesgo Potencial	13
2.4.2 Riesgo Residual	16
2.4.3 Riesgo Objetivo	17
3. Conclusiones	22
Anexo I – Inventario de Activos	24
Inventario de Activos	24
Clases de Activos	25
Dependencias entre Activos	35
Valoración del Servicio Radar Covid19	36
Anexo II – Criterios de Valoración de las Dimensiones de Seguridad	38
Anexo III – Caracterización de Salvaguardas	40
Madurez ENS	40
Madurez RGPD	42
Anexo IV – Información Modificada de Amenazas	59

1. Introducción

El análisis de riesgos es un requisito recogido en el Real Decreto 951/2015, de 23 de octubre, de modificación del Real Decreto 3/2010, de 8 de enero, por el que se regula el **Esquema Nacional de Seguridad (ENS)** en el ámbito de la administración electrónica.

Los siguientes artículos del Esquema Nacional de Seguridad hacen referencia a la importancia y necesidad de realizar un análisis de riesgos:

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. *El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.*
2. *La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.*

Artículo 13. Análisis y gestión de los riesgos.

1. *Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.*
2. *Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el anexo II, se empleará alguna metodología reconocida internacionalmente.*
3. *Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.*

Además la obligatoriedad de realizar un análisis de riesgos se encuentra recogida en:

- La **medida op.pl.1** del marco operacional del Anexo II del Esquema Nacional de Seguridad, como una de las medidas de seguridad que es necesario implantar para los sistemas de información a partir de una categoría Básica.

Marco operacional [op]. Análisis de riesgos [op.pl.1].

Categoría BÁSICA

Bastará un análisis informal, realizado en lenguaje natural. Es decir, una exposición textual que describa los siguientes aspectos:

- a) *Identifique los activos más valiosos del sistema.*
- b) *Identifique las amenazas más probables.*
- c) *Identifique las salvaguardas que protegen de dichas amenazas.*
- d) *Identifique los principales riesgos residuales.*

Categoría MEDIA

Se deberá realizar un análisis semi-formal, usando un lenguaje específico, con un catálogo básico de amenazas y una semántica definida. Es decir, una presentación con tablas que describa los siguientes aspectos:

- a) *Identifique y valore cualitativamente los activos más valiosos del sistema.*
- b) *Identifique y cuantifique las amenazas más probables.*
- c) *Identifique y valore las salvaguardas que protegen de dichas amenazas.*
- d) *Identifique y valore el riesgo residual.*

Categoría ALTA

Se deberá realizar un análisis formal, usando un lenguaje específico, con un fundamento matemático reconocido internacionalmente. El análisis deberá cubrir los siguientes aspectos:

- a) *Identifique y valore cualitativamente los activos más valiosos del sistema.*
- b) *Identifique y cuantifique las amenazas posibles.*

- c) *Identifique las vulnerabilidades habilitantes de dichas amenazas.*
- d) *Identifique y valore las salvaguardas adecuadas.*
- e) *Identifique y valore el riesgo residual.*

- El **apartado 1. Objeto de la Auditoría** del Anexo III Auditoría de seguridad del Esquema Nacional de Seguridad, donde se indica:
1.1 La seguridad de los sistemas de información de una organización será auditada en los siguientes términos:

-
- d) *Que se ha realizado un análisis de riesgos, con revisión y aprobación anual.*
-

1.1 Objetivos

El presente documento tiene como objetivo exponer los resultados del Análisis de Riesgos realizado al **Servicio Radar Covid19** respecto al Esquema Nacional de Seguridad.

El Análisis de Riesgos debe ser realizado y aprobado anualmente, y será objeto de auditoría tal y como se indica en el Anexo III del Real Decreto 3/2010.

1.2 Alcance

El presente Análisis de Riesgos se ha realizado sobre la infraestructura que se encuentra detallada en el documento “*App Bluetooth contra Covid-19 v5.pdf*” y que es necesaria para prestar el **Servicio Radar Covid19** de la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA).

Cualquier otra aplicación o infraestructura necesaria para llevar a cabo el *Servicio Radar Covid19* que no esté dentro del alcance especificado no ha sido tomada en cuenta en este análisis de riesgos.

1.3 Estructura del documento

El documento se estructura de la siguiente forma:

- Introducción: Es el presente apartado, donde se establecen los objetivos del documento, el alcance, la estructura del documento y las Referencias documentales.
- Metodología de Análisis de Riesgos: Identificación de la Fase de desarrollo del Plan de Adecuación al ENS y descripción de las tareas de la Metodología MAGERIT, utilizada para realizar las actividades y tareas del Análisis de Riesgos y la descripción del trabajo realizado:
 - Categorización de Activos
 - Categorización de Amenazas
 - Categorización de Salvaguardas
 - Estimación del Estado del Riesgo
- Conclusiones: Resultados y principales conclusiones y recomendaciones del Análisis de Riesgos.
- Anexos: Información complementaria al presente documento.

1.4 Referencias Documentales

- Real Decreto 3/2010, de 8 de enero, modificado por el Real Decreto 951/2015, de 23 de octubre, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.
- Ley Orgánica 3/2018, de 5 de diciembre, de Protección de Datos Personales y garantía de los derechos digitales.
- MAGERIT (Versión 3.0), Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
- Guías STIC de Seguridad de la Serie 800 (Esquema Nacional de Seguridad) elaboradas por el Centro Criptológico Nacional)

2. Metodología de Análisis de Riesgos

El Análisis de Riesgos constituye una de las Fases del Plan de Adecuación al ENS, como se muestra el esquema que sigue a continuación:

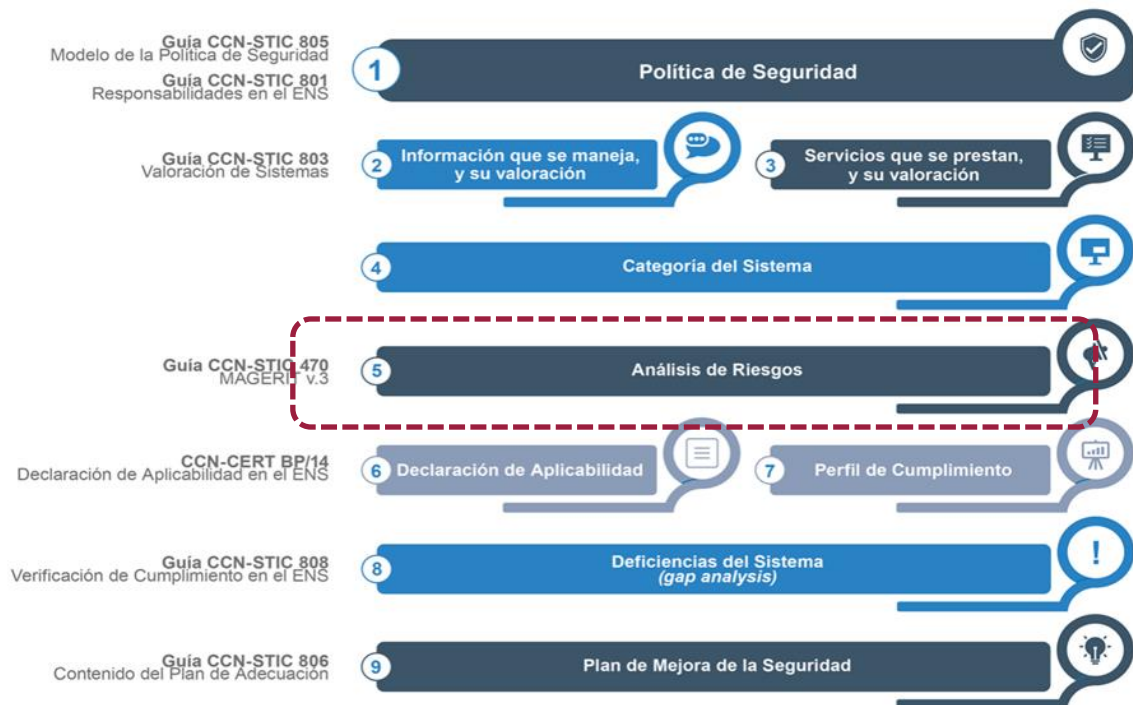


Ilustración 1 Plan de Adecuación al ENS

Para la realización del Análisis de Riesgos se han mantenido diferentes reuniones con los responsables técnicos involucrados en el Desarrollo e implantación de la **Aplicación Radar Covid19**. Como resultado de esta actividad se ha recopilado la información descrita en la Metodología MAGERIT y requerida por la Herramienta PILAR.

Las fases del análisis de riesgos se basan en los hitos de control definidos en MAGERIT.

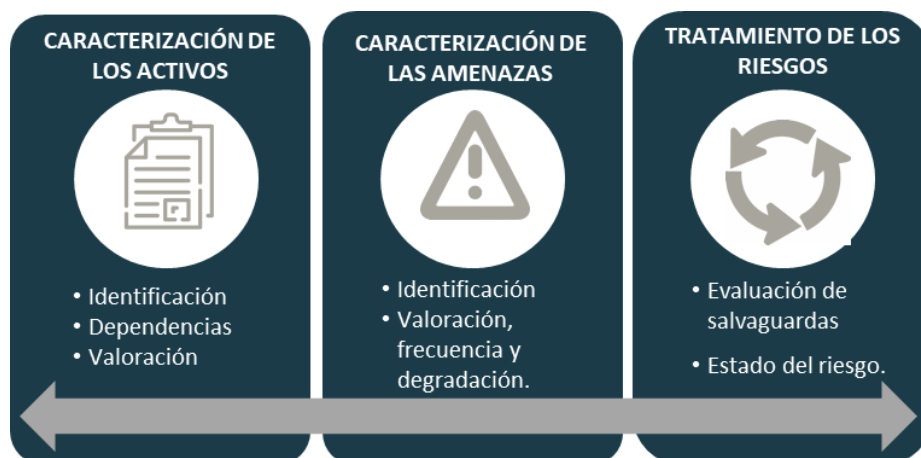


Ilustración 2 Fases del Análisis de Riesgos

MAGERIT describe las siguientes actividades para desarrollar el Análisis de Riesgos:

- **Caracterización de activos.** Identificación y valoración de los activos que forman parte del alcance del Análisis de Riesgos. La valoración se realiza de acuerdo a las dimensiones de seguridad: Autenticidad, Confidencialidad, Integridad, Disponibilidad y Auditabilidad o Trazabilidad, referidas en este informe como valoración ACIDA.
- **Caracterización de amenazas.** Identificación de las amenazas a las que están expuestos los activos, caracterizándolas por las estimaciones de ocurrencia (probabilidad) y daño causado (degradación). De este modo es posible estimar el riesgo potencial o intrínseco sobre cada uno de los activos.
- **Tratamiento de los Riesgos – Evaluación de salvaguardas.** Identificación de las salvaguardas desplegadas actualmente, calificándolas por su eficacia frente a las amenazas que pretenden mitigar. Para caracterizar las salvaguardas se ha utilizado como referencia el Anexo II: Medidas de Seguridad, del Esquema Nacional de Seguridad (RD 951/2015).
- **Tratamiento de los Riesgos - Estado del Riesgo.** Teniendo en cuenta la información relativa a la caracterización de Activos, Amenazas y Salvaguardas, se determina la variación del riesgo desde un valor potencial a un valor actual o residual.

2.1 Caracterización de Activos

Mediante esta actividad se ha procedido a **identificar** los activos que forman parte del alcance del Análisis de Riesgos y que son susceptibles de ser atacados deliberada o accidentalmente con consecuencias negativas para la Organización. La relación de Activos se recoge en el [Anexo I: Inventario de Activos](#), de los cuales, como se puede observar, se ha calificado como **Activo Esencial** el **Servicio [0001] Servicio Radar Covid19**, sobre el que además se ha incorporado toda la información relativa al RGPD.

El anexo mencionado anteriormente recoge también la **caracterización** o tipología de cada uno de ellos, así como las **dependencias** entre activos. Esta información es la utilizada por la Herramienta PILAR para asociar las amenazas por tipo de activo.

Una vez identificados los activos esenciales se ha realizado la **valoración** de los mismos, de acuerdo a la información disponible sobre el **Servicio Radar Covid19** en relación con las Dimensiones de Seguridad:

- **Autenticidad:** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Confidencialidad:** Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Integridad:** Propiedad o característica consistente en que el activo de información no ha sido alterado de manera no autorizada.
- **Disponibilidad:** Propiedad o característica de los activos, consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Auditabilidad o Trazabilidad:** Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad.

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: Criterios de Valoración de Sistemas de Información](#).

La valoración se ha determinado teniendo en cuenta la Guía CCN-STIC 803 ENS “*Valoración de los sistemas*”. Esta valoración junto a su justificación se encuentra detallada en el [Anexo I: Inventario de Activos](#).

Una vez que se han identificado los activos, es necesario establecer la relación de dependencia que tienen entre ellos. La ilustración que sigue a continuación muestra un esquema simplificado de las relaciones establecidas en el Análisis de Riesgos.

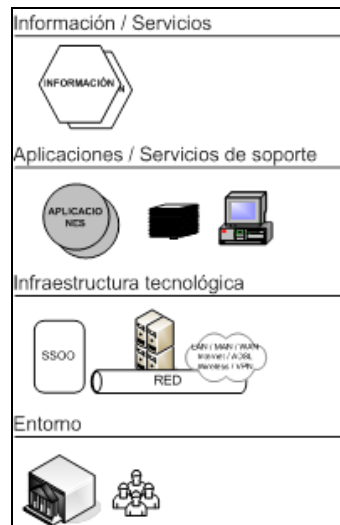


Ilustración 3 Dependencias básicas de Activos

En el apartado “Dependencias entre Activos” del [Anexo I: Inventario de Activos](#) se muestran las dependencias establecidas para el **Servicio Radar Covid19**.

2.2 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.

Las amenazas representan eventos que pueden desencadenar un incidente de seguridad, produciendo daños materiales o pérdida de información. La diversidad de posibles orígenes o causas de las amenazas permite clasificar estas según su naturaleza. El Libro II de MAGERIT V3.0 “*Catálogo de elementos*” (Capítulo 5: Amenazas) incluye la relación de amenazas que se ha considerado para el presente Análisis de Riesgos y que constituye el catálogo de amenazas implementadas de forma estándar en la Herramienta PILAR. A continuación se describen brevemente las categorías de amenazas consideradas en dicho catálogo:

- *Desastres naturales [N.*]*: Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta. Existen accidentes naturales ante los cuales el sistema de información es víctima pasiva, no obstante, hay que tener en cuenta sus posibles consecuencias.
- *De origen industrial [I.*]*: Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Al igual que en el caso anterior es necesario tener en cuenta sus posibles consecuencias.
- *Errores y fallos no intencionados [E.*]*: Fallos no intencionales causados por las personas. Por su naturaleza, este tipo de amenazas pueden afectar a cualquiera de las dimensiones de seguridad.
- *Ataques intencionados [A.*]*: Ataques deliberados causados por las personas. Por su naturaleza, este tipo de amenazas también pueden afectar a cualquiera de las dimensiones de seguridad.

No todas las amenazas afectan a todos los activos, sino que existe una relación entre el tipo de activo y lo que le podría ocurrir. Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni con la misma gravedad. 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 %	El activo queda totalmente inutilizado, causando un daño excepcional sobre su misión para la Organización
90 %	El activo ha sufrido importantes daños, que muy probablemente tengan serias repercusiones sobre su misión en la Organización.
50%	Aunque la degradación ha sido importante, el activo (o un respaldo suyo) puede seguir funcionando.
10 %	Se producen daños en el activo que pueden causar pérdidas menores o mermas en la seguridad sobre ciertos aspectos.
1 %	La degradación sería causa de inconveniencias mínimas sobre la Organización.

Tabla 1 Degradación de Activos

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

Tabla 2 Frecuencia de Amenazas

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 Covid19**. Dichas modificaciones se recogen en el [Anexo IV: Información Modificada de Amenazas](#).

A continuación se presenta, a modo ejemplo, una captura de pantalla de la Herramienta PILAR que muestra la asociación de amenazas para el activo [SW0001] App Radar Covid19, indicando la dimensión que resultaría degradada y con qué frecuencia.

[001] A.3.3. valoración

Editar Exportar Importar TSV

activo	co...	frecuencia	[D]	[I]	[C]	[A]	[T]	[V]	[DP]
ACTIVOS									
[B] Activos esenciales									
[E] Equipamiento									
[SW] Aplicaciones									
[SW-0001] App Radar Covid19									
A									
[L5] Avería de origen físico o lógico		1	A						
[E.8] Difusión de software dañino		1	M	M	M				
[E.20] Vulnerabilidades de los programas (software)		1	B	M	M				
[E.21] Errores de mantenimiento / actualización de programas		1	B	B					
[A.8] Difusión de software dañino		1	T	T	T				
[A.22] Manipulación de programas		1	A	T	T				
[HW] Equipos									
[COM] Comunicaciones									
[SP] SOPORTES									
[SS] Servicios Subcontratados									
[SE] Servicios Externos									
[I.] Instalaciones									
[P] Personal									

Ilustración 4 Asociación de Amenazas-Activos

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 v2.1.mgr**.

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

2.3 Evaluación de Salvaguardas

En las fases anteriores no se han tomado en consideración las salvaguardas desplegadas, es decir, el riesgo potencial no tiene en cuenta las medidas de protección.

Se definen las salvaguardas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se minimizan simplemente con una organización adecuada, otras requieren elementos técnicos (programas o equipos), otras requieren seguridad física, política de personal, etc.

Existen múltiples catálogos de salvaguardas que cubren los aspectos más diversos de los sistemas de información. MAGERIT no exige la utilización de ningún catálogo en particular, pero incluye en su anexo "Catálogo de Elementos" una relación de salvaguardas genéricas. La Herramienta PILAR soporta este catálogo y otros como el estándar internacional ISO/IEC 27002 Código de buenas prácticas para la Gestión de la Seguridad de la Información, las medidas de seguridad de protección de datos de carácter personal (GDPR) y las medidas de implantación del Esquema Nacional de Seguridad (ENS).

En este caso y como el Análisis de Riesgos se está realizando respecto al Esquema Nacional de Seguridad, se ha utilizado el catálogo de salvaguardas del ENS, implementado por la Herramienta PILAR. Estas salvaguardas se corresponden con las medidas exigidas por el ENS en su Anexo II. Además se ha incorporado el catálogo de salvaguardas del RGPD implementado por la Herramienta PILAR.

La siguiente tabla resume el conjunto de medidas de seguridad recogidas en el Anexo II del Esquema Nacional de Seguridad:

Marco Organizativo	Marco Operacional	Medidas de protección
Política de seguridad	Planificación	Protección de las instalaciones e infraestructuras
Normativa de seguridad	Control de accesos	Gestión del personal
Procedimientos de seguridad	Explotación	Protección de los equipos
Proceso de autorización	Servicios Externos	Protección de las comunicaciones
	Continuidad del Servicio	Protección de los soportes de información
	Monitorización del sistema	Protección de las aplicaciones informáticas
		Protección de la información
		Protección de los servicios

Tabla 3 Medidas de Seguridad del ENS

Como se puede observar, las medidas de seguridad contempladas se pueden clasificar en los siguientes grupos:

- **Marco organizativo:** Medidas relacionadas con la organización global de la seguridad.
- **Marco operacional:** Medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.
- **Medidas de protección:** Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

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	<i>Inexistente (0 %)</i> Esta medida no existe o no está siendo aplicada en este momento.
L1	<i>Inicial / Ad Hoc (10 %)</i> La organización no proporciona un entorno estable. El proceso existe pero no se gestiona. 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	<i>Reproducible pero Intuitivo (50%) o Parcialmente Realizado</i>

Nivel de Madurez	Descripción
	<p>La eficacia del proceso depende del grado de conocimiento de cada individuo.</p> <p>Los procesos similares se llevan en forma similar por diferentes personas. Es impredecible el resultado si se dan circunstancias nuevas.</p> <p>Se normalizan las buenas prácticas en base a la experiencia. No hay comunicación o entrenamiento formal, las responsabilidades quedan a cargo de cada individuo.</p>
L3	<p><i>Proceso Definido (90 %) o En Funcionamiento</i></p> <p>Los procesos están implantados, documentados y comunicados mediante entrenamiento.</p> <p>La Organización entera participa en el proceso y existe una coordinación entre departamentos.</p>
L4	<p><i>Gestionado y Medible (95 %) o Monitorizado</i></p> <p>Se dispone de un sistema de medidas y métricas para conocer el desempeño (eficacia y eficiencia) de los procesos.</p> <p>Se dispone de la tecnología adecuada para automatizar el flujo de trabajo, se tienen herramientas para mejorar la calidad y la eficiencia.</p> <p>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.</p>
L5	<p><i>Optimizado (100 %)</i></p> <p>Se centra en la mejora continua de los procesos con mejoras tecnológicas incrementales e innovadoras.</p> <p>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.</p>

Tabla 4 Niveles de Madurez

La caracterización de las salvaguardas se ha realizado mediante reuniones con los responsables técnicos de Radar COVID, responsables del desarrollo, puesta en marcha e implantación de la **Aplicación Radar Covid19**, 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: 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 han mantenido reuniones para identificar el grado de madurez de cada uno de los artículos del RGPD.

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: Caracterización de las Salvaguardas*.

A continuación, a modo de resumen, se muestra el grado de madurez de las medidas de seguridad del ENS, mediante la siguiente gráfica:

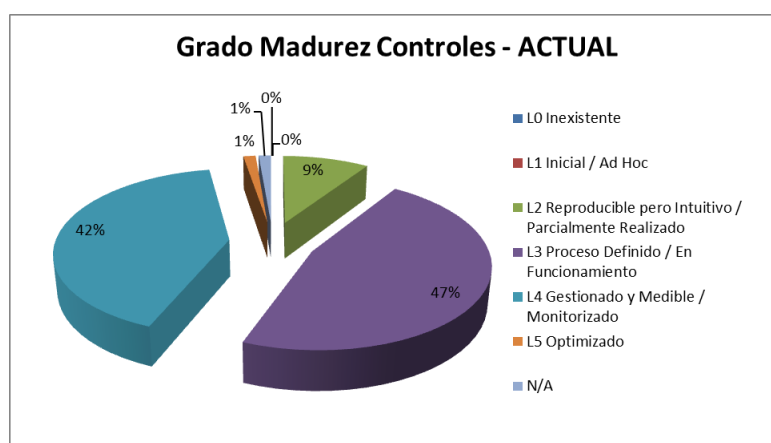


Ilustración 5 Grado de Madurez de los Controles ENS – Actual

2.4 Estado del Riesgo

Se entiende como riesgo la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos, causando daños o perjuicios a la Organización. El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente.

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 5 Escala de Valores de Riesgo

2.4.1 Riesgo Potencial

Es la medida del riesgo que se obtiene cuando no se considera salvaguarda alguna de protección. Es un escenario inicial que servirá para estimar la mejora que supone implantar medidas de protección.

Tomando como métrica para el nivel de riesgo en cada activo, el mayor valor de riesgo identificado en ese activo, se obtiene el siguiente ranking de **riesgos potenciales** asociados a cada activo dentro del alcance:

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

Tabla 6 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:

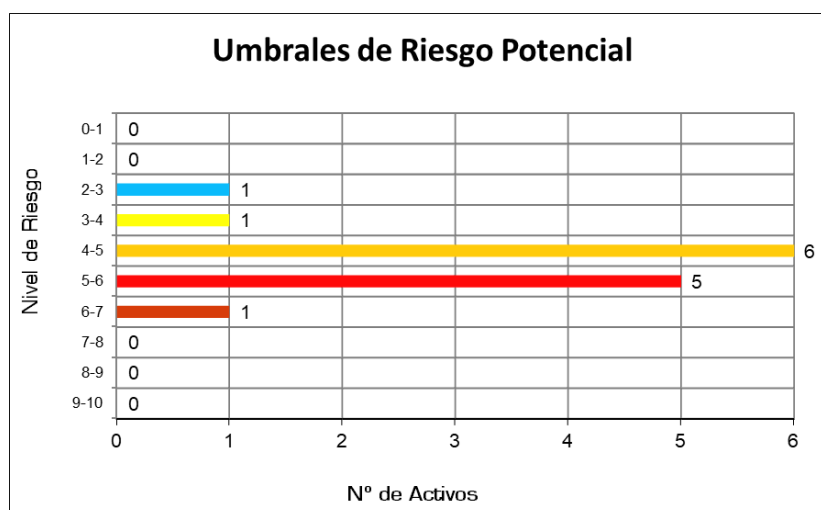


Ilustración 6 Número de Activos por nivel de Riesgo Potencial

La gráfica muestra que hay 1 activo con riesgo muy crítico, 5 con riesgo crítico, 6 con riesgo muy alto, 1 con riesgo alto y 1 con riesgo medio.

A continuación se indican las amenazas de están afectando a los activos cuyo riesgo es Muy Alto, Crítico o Muy Crítico:

[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 fácil					4,1	4,1
[COM-0001] Redes de Comunicaciones	5,1	4,5	5,3	3,8		5,3
[A.11] Acceso no autorizado	5,1	4,5	3,3	3,3		5,1
[A.18] Destrucción de la información			4,5			4,5
[A.23] Manipulación del hardware		4,3	4,8			4,8
[A.24] Denegación de servicio			5,3			5,3
[A.26] Ataque destructivo			4,2			4,2
[A.5] Suplantación de la identidad	4,2	3,7		2,4		4,2
[E.24] Caída del sistema por agotamiento de recursos			4,5			4,5
[E.25] Pérdida de equipos		4,5	3,8			4,5
[I.1] Fuego			4,2			4,2
[I.6] Corte del suministro eléctrico			4,2			4,2
[I.7] Condiciones inadecuadas de temperatura o humedad			4,2			4,2
[I.8] Fallo de servicios de comunicaciones			4,5			4,5
[N.1] Fuego			4,2			4,2
[SW-0001] App Radar Covid19	5,1	5,1	5,1			5,1
[A.22] Manipulación de programas		5,1	4,5	5,1		5,1
[A.8] Difusión de software dañino		5,1	5,1	5,1		5,1
[I.5] Avería de origen físico o lógico			4,5			4,5
[P-0002] Administradores / Operadores	4,8	4,3	4,8			4,8
[A.28] Indisponibilidad del personal			4,3			4,3
[A.29] Extorsión		4,2	3,7	4,2		4,2
[A.30] Ingeniería social (picaresca)		4,8	4,3	4,8		4,8
[P-0003] Desarrolladores	4,2	3,6	4,2			4,2
[A.29] Extorsión		4,2	2,4	4,2		4,2
[A.30] Ingeniería social (picaresca)		4,2	2,4	4,2		4,2
[SS-0001] Desarrollo y Mantenimiento de la App	4,2	4,2	3,7	4,2	4,2	4,2
[A.13] Repudio (negación de actuaciones)					4,2	4,2
[A.5] Suplantación de la identidad	4,2	4,2		4,2		4,2
[SP-0001] Soportes		5,1	5,1	5,7		5,7
[A.11] Acceso no autorizado		4,5		1,5		4,5
[A.15] Modificación de la información				5,7		5,7
[A.18] Destrucción de la información			5,1			5,1
[A.25] Robo de equipos		5,1	3,3			5,1
[E.18] Destrucción de la información			5,1			5,1
[E.23] Errores de mantenimiento / actualización de equipos (hardware)			5,1			5,1
[E.25] Pérdida de equipos		4,5	3,3			4,5
[I.*] Desastres industriales			4,8			4,8
[I.1] Fuego			4,8			4,8
[I.10] Degradación de los soportes de almacenamiento de la información			5,1			5,1
[I.2] Daños por agua			4,3			4,3
[I.3] Contaminación medioambiental			4,5			4,5
[I.5] Avería de origen físico o lógico			4,5			4,5
[I.6] Corte del suministro eléctrico			5,1			5,1
[I.7] Condiciones inadecuadas de temperatura o humedad			5,1			5,1
[N.*] Desastres naturales			4,2			4,2
[N.1] Fuego			4,2			4,2
[HW-0002] Equipos AWS		5,1	5,1	5,1		5,1
[A.11] Acceso no autorizado		5,1	3,3	5,1		5,1
[A.23] Manipulación del hardware		4,3	4,3			4,3
[A.24] Denegación de servicio			5,1			5,1
[A.25] Robo de equipos		4,2	4,2			4,2
[A.26] Ataque destructivo			4,2			4,2
[A.6] Abuso de privilegios de acceso		5,1	3,3	5,1		5,1
[A.7] Uso no previsto		5,1	3,3	3,3		5,1
[E.24] Caída del sistema por agotamiento de recursos			4,5			4,5
[E.25] Pérdida de equipos		5,1	5,1			5,1
[I.1] Fuego			4,2			4,2
[I.6] Corte del suministro eléctrico			4,2			4,2
[I.7] Condiciones inadecuadas de temperatura o humedad			4,2			4,2
[N.1] Fuego			4,2			4,2
[L-0001] Instalaciones AWS		4,5	5,1	3,3		5,1
[A.11] Acceso no autorizado		4,5		3,3		4,5
[A.23] Manipulación del hardware		4,5	4,5			4,5
[A.25] Robo de equipos			5			5
[A.26] Ataque destructivo			5,1			5,1
[A.7] Uso no previsto		1,5	4,5	1,5		4,5
[I.*] Desastres industriales			4,8			4,8
[I.1] Fuego			4,8			4,8
[I.2] Daños por agua			4,8			4,8
[N.*] Desastres naturales			4,2			4,2
[N.1] Fuego			4,2			4,2
[N.2] Daños por agua			4,2			4,2
[SE-0002] Repositorio Descargas (APPLE STORE)	4,2	4,2	3,7	4,2	4,2	4,2
[A.13] Repudio (negación de actuaciones)					4,2	4,2
[A.5] Suplantación de la identidad	4,2	4,2		4,2		4,2
[SS-0002] Servicio Cloud	4,2	4,2	3,7	4,2	4,2	4,2
[A.13] Repudio (negación de actuaciones)					4,2	4,2
[A.5] Suplantación de la identidad	4,2	4,2		4,2		4,2
[SE-0001] Repositorio Descargas (ANDROID STORE)	4,2	4,2	3,7	4,2	4,2	4,2
[A.13] Repudio (negación de actuaciones)					4,2	4,2
[A.5] Suplantación de la identidad	4,2	4,2		4,2		4,2

Ilustración 7 Amenazas para los activos con riesgos Muy Alto, Crítico o Muy Crítico

2.4.2 Riesgo Residual

El riesgo residual es el resultado de caracterizar las amenazas a las que están expuestos los activos y determinar la eficacia de las salvaguardas actualmente desplegadas.

Tomando como métrica para el nivel de riesgo en cada activo, el mayor valor de riesgo identificado en ese activo, se obtiene el siguiente ranking de **riesgos residuales** asociados a cada activo dentro del alcance:

Activos	Riesgo Residual
[001] Servicio Radar Covid19	2,6
[SP-0001] Soportes	1
[L-0001] Instalaciones AWS	0,9
[HW-0002] Equipos AWS	0,9
[SW-0001] App Radar Covid19	0,9
[COM-0001] Redes de Comunicaciones	0,9
[SS-0002] Servicio Cloud	0,8
[SE-0002] Repositorio Descargas (APPLE STORE)	0,8
[SE-0001] Repositorio Descargas (ANDROID STORE)	0,8
[P-0002] Administradores / Operadores	0,8
[SS-0001] Desarrollo y Mantenimiento de la App	0,8
[P-0003] Desarrolladores	0,6
[P-0001] Ciudadanos	0,5
[HW-0001] Teléfono Móvil	0,4
Total general	2,6

Tabla 7 Riesgo Residual

A continuación 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:

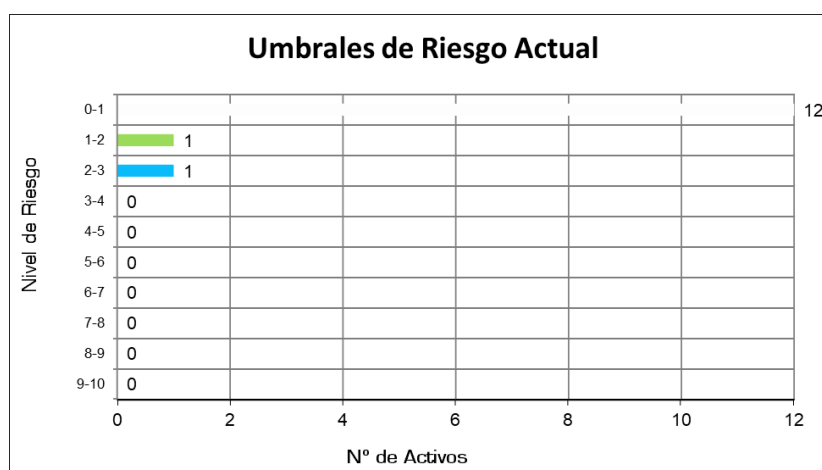


Ilustración 8 Número de Activos por nivel de Riesgo Residual

Como puede observarse, una vez que se han tenido en cuenta las salvaguardas implantadas, el nivel de riesgo de los activos se reduce considerablemente. En la gráfica se puede observar que hay 12 activos con riesgo despreciable, 1 con riesgo bajo y 1 con riesgo medio.

A continuación se indican las amenazas de están afectando al activo con riesgo Medio:

Activo / Amenaza	A	C	D	I	T	DP	Máximo
[001] Servicio Radar Covid19	2,6	2,6	0,4	1,5		0,8	2,6
[A.11] Acceso no autorizado		2,6		1,5			2,6
[A.5] Suplantación de la identidad	2,6	1,9		0,9			2,6

Ilustración 9 Amenazas para los activos con riesgo Medio

2.4.3 Riesgo Objetivo

El proceso de Análisis de Riesgos permite conocer las principales debilidades existentes en los Sistemas de Información, sirviendo de base para diseñar un *Plan de Tratamiento de Riesgos*. Es por ello que el Análisis de Riesgos debe dar paso a un proceso de gestión del riesgo, que consiste en definir y planificar las acciones adecuadas de mejora teniendo en cuenta los resultados de dicho análisis.

Este plan debería incluir la implantación de salvaguardas no implantadas hasta el momento o que no se encuentran en el grado de madurez exigido por el ENS. La guía de Implantación ENS, CCN-STIC-804, en su apartado 2 indica lo siguiente:

Como regla general, se exigirá un nivel de madurez en las medidas de seguridad en proporción al nivel de las dimensiones afectadas o de la categoría del sistema:

Nivel de madurez medidas de seguridad	Categoría del sistema de las tecnologías de la información y la comunicación	Nivel de madurez mínimo exigido
Bajo	Básica	L2 - Repetible, pero intuitivo
Medio	Media	L3 - Proceso definido
Alto	Alta	L4 - Gestionado y medible

Ilustración 10 Niveles madurez exigidos en función Categoría del Sistema

Por lo que para el Sistema de Información del **Servicio Radar Covid19** que presenta una categoría **ALTA**, le corresponde un **nivel L4**.

El detalle del nivel de madurez mínimo exigido por el Esquema Nacional de Seguridad para cada medida de seguridad se puede ver en detalle en la Guía CCN-STIC 824: *Informe Nacional del Estado de Seguridad de los Sistemas TIC*.

La Herramienta PILAR realiza una propuesta del grado de madurez que debe tener cada una de las medidas de seguridad según el Esquema Nacional de Seguridad, que en este caso es inferior al grado de madurez que tienen las medidas de seguridad para el Servicio Radar Covid19. La siguiente imagen muestra el grado de madurez (en porcentaje) para cada grupo de medidas de seguridad (marco organizativo, marco operaciones y medidas de protección) que está implantado actualmente para el Servicio Radar Covid19 contrastándolo con el que propone la Herramienta PILAR para el ENS:

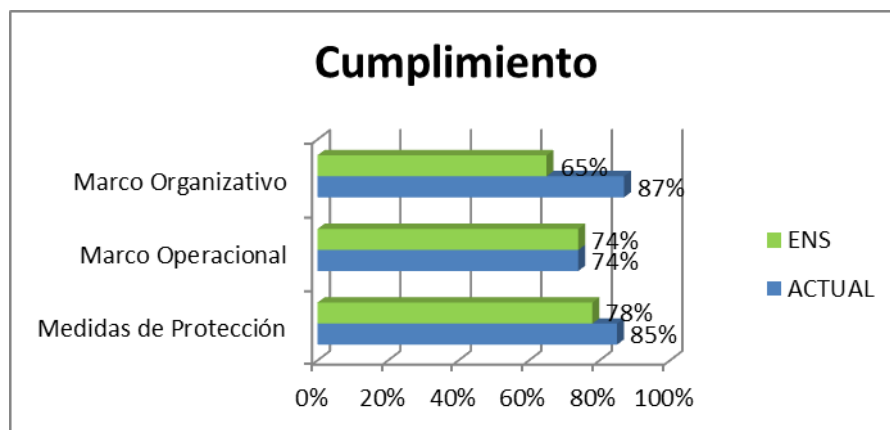


Ilustración 11 Grado de madurez Actual y ENS

Para realizar este Plan de 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 Covid19* todos los riesgos han salido por debajo del valor {3}, siendo el riesgo residual identificado más alto de nivel MEDIO cuyo valor es {2,6}.

Para el *Servicio Radar Covid19* se ha propuesto realizar las 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.

La siguiente imagen muestra el activo junto a las amenazas que le hacen tener un riesgo por encima del valor {2} MEDIO.

Activo / Amenaza	A	C	D	I	T	DP	Máximo
[001] Servicio Radar Covid19	2,6	2,6	0,4	1,5		0,8	2,6
[A.11] Acceso no autorizado		2,6		1,5			2,6
[A.5] Suplantación de la identidad	2,6	1,9		0,9			2,6

Ilustración 12 Amenazas para los activos con riesgo Medio

Se recomienda abordar un conjunto de acciones para mejorar las medidas de seguridad existentes actualmente, con el objeto de ajustar el nivel de riesgo del *Servicio Radar Covid19* a un nivel BAJO. Estas acciones se han focalizado en las medidas que pueden minimizar las amenazas que aportan un riesgo MEDIO en el presente Análisis de Riesgos.

Estas acciones permitirán alcanzar el nivel de Riesgo Objetivo propuesto ya que aumentarían el grado de madurez de las siguientes medidas de seguridad:

- **Mp.info.4 Firma electrónica:** La medida de seguridad de firma electrónica establece que: *"Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la autenticidad de la procedencia y la integridad de la información ofreciendo las bases para evitar el repudio. La integridad y la autenticidad de los documentos se garantizarán por medio de firmas electrónicas con los condicionantes que se describen a continuación, proporcionados a los niveles de seguridad requeridos por el sistema. En el caso de que se utilicen otros mecanismos de firma electrónica sujetos a derecho, el sistema debe incorporar medidas compensatorias suficientes que ofrezcan garantías equivalentes o superiores en lo relativo a prevención del repudio, usando el procedimiento previsto en el punto 5 del artículo 27".*

Para esta medida de seguridad teniendo en cuenta la valoración en cada una de las dimensiones de seguridad dada al **Servicio Radar Covid19**, se deben tomar en cuenta

los niveles de salvaguarda de manera acumulativa, es decir, que se deben aplicar la medidas recomendadas desde el nivel bajo hasta el alto, para su protección, la descripción de estos niveles viene dada a continuación:

“Nivel BAJO

Se empleará cualquier tipo de firma electrónica de los previstos en la legislación vigente.

Nivel MEDIO

- a. *Cuando se empleen sistemas de firma electrónica avanzada basados en certificados, estos serán cualificados.*
- b. *Se emplearán algoritmos y parámetros acreditados por el Centro Criptológico Nacional.*
- c. *Se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la Política de Firma Electrónica y de Certificados que sea de aplicación. Para tal fin:*
- d. *Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación: 1. Certificados. 2. Datos de verificación y validación.*
- e. *El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes 1 y 2 del apartado d).*
- f. *La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes 1 y 2.*

Nivel ALTO

1. *Se usará firma electrónica cualificada, incorporando certificados cualificados y dispositivos cualificados de creación de firma.*
2. *Se emplearán productos certificados conforme a lo establecido en [op.pl.5].”*

El nivel de madurez identificado para esta medida ha sido *L2 Repetible, pero intuitivo*; ya que según se expone “No se han utilizado certificados cualificados de firma electrónica.” Para proporcionar mayor seguridad se propone la utilización de **certificados cualificados** para la firma digital que se utiliza en el **servicio de verificación de los positivos**.

- **Op.acc.5 Mecanismos de autenticación.** En el caso de los resultados obtenidos para la medida de seguridad Mecanismos de autenticación, la cual establece que: “*los mecanismos de autenticación frente al sistema se adecuarán al nivel del sistema atendiendo a las consideraciones que siguen, pudiendo usarse los siguientes factores de autenticación: – “algo que se sabe”: contraseñas o claves concertadas. – “algo que se tiene”: componentes lógicos (tales como certificados software) o dispositivos físicos (en expresión inglesa, tokens). – “algo que se es”: elementos biométricos. Los factores anteriores podrán utilizarse de manera aislada o combinarse para generar mecanismos de autenticación fuerte. Las guías CCN-STIC desarrollarán los mecanismos concretos adecuados para cada nivel. Las instancias del factor o los factores de autenticación que se utilicen en el sistema, se denominarán credenciales. Antes de proporcionar las credenciales de autenticación a los usuarios, estos deberán haberse identificado y registrado de manera fidedigna ante el sistema o ante un proveedor de identidad electrónica reconocido por la Administración. Se contemplan varias posibilidades de registro de los usuarios: – Mediante la presentación*

física del usuario y verificación de su identidad acorde a la legalidad vigente, ante un funcionario habilitado para ello. – De forma telemática, mediante DNI electrónico o un certificado electrónico cualificado. – De forma telemática, utilizando otros sistemas admitidos legalmente para la identificación de los ciudadanos de los contemplados en la normativa de aplicación.

Para un **Nivel ALTO**, como el que se le ha atribuido al *Servicio Radar Covid19*, se dispone que:

- a. *Las credenciales se suspenderán tras un periodo definido de no utilización.*
- b. *En el caso del uso de utilización de "algo que se tiene", se requerirá el uso de elementos criptográficos hardware usando algoritmos y parámetros acreditados por el Centro Criptológico Nacional.*
- c. *Las credenciales utilizadas deberán haber sido obtenidas tras un registro previo presencial o telemático usando certificado electrónico cualificado en dispositivo cualificado de creación de firma.*

El nivel de madurez identificado para esta medida ha sido: L2 - Repetible, pero intuitivo, ya que aunque el acceso a la consola de AWS se realiza mediante *AWS Multi-Factor Authentication (MFA)*, y por tanto cumple con la medida de utilizar un segundo factor de autenticación, se recomienda verificar que los elementos criptográficos hardware utilizan algoritmos y parámetros acreditados por el CCN. Además se recomienda revisar el mecanismo control de acceso a la Base de Datos PostgreSQL para concluir que cumple con los requisitos de nivel alto.

El **riesgo objetivo**, una vez realizadas estas acciones disminuye, quedando como sigue:

Activos	Riesgo Objetivo
[001] Servicio Radar Covid19	1,8
[SP-0001] Soportes	1
[L-0001] Instalaciones AWS	0,9
[HW-0002] Equipos AWS	0,9
[SW-0001] App Radar Covid19	0,9
[COM-0001] Redes de Comunicaciones	0,9
[SS-0002] Servicio Cloud	0,8
[SE-0002] Repositorio Descargas (APPLE STORE)	0,8
[SE-0001] Repositorio Descargas (ANDROID STORE)	0,8
[P-0002] Administradores / Operadores	0,8
[SS-0001] Desarrollo y Mantenimiento de la App	0,8
[P-0003] Desarrolladores	0,6
[P-0001] Ciudadanos	0,5
[HW-0001] Teléfono Móvil	0,4
Total general	1,8

Tabla 8 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:

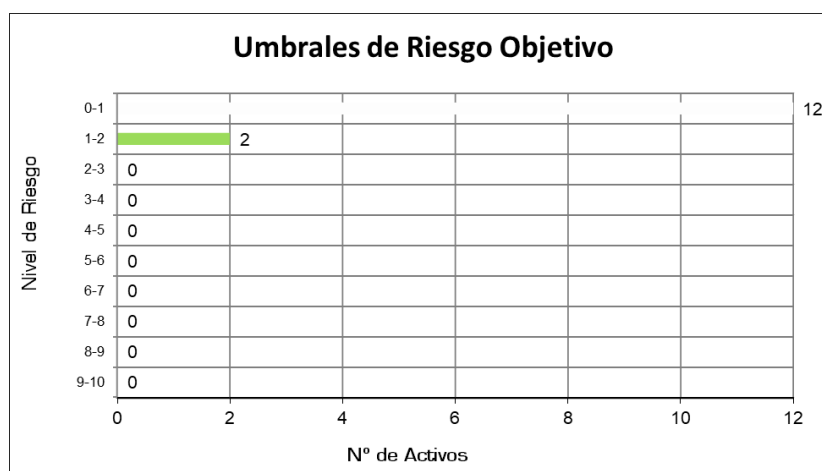


Ilustración 13 Número de Activos por nivel de Riesgo Objetivo

Como puede observarse, una vez que se realicen las acciones propuestas, 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.

3. Conclusiones

El principal objetivo del Análisis de Riesgos es determinar el nivel de riesgo al que están expuestos los activos del **Servicio Radar Covid19**, teniendo en cuenta las amenazas a las que están expuestos y el nivel de eficacia de los controles implantados actualmente para protegerlos.

El Análisis de Riesgos está basado en la información aportada por los responsables técnicos y los responsables del desarrollo, puesta en marcha e implantación de la **Aplicación Radar Covid19**, quienes conocen la infraestructura y que, por tanto, pueden conocer el grado de implantación de cada una de las medidas de seguridad del Anexo II del Esquema Nacional de Seguridad.

Por otra parte, el presente documento se ha elaborado con la información recabada hasta su fecha de edición, por lo que, salvo indicación expresa, los cambios realizados después de esta fecha no se verán reflejados en el mismo.

Como se ha comentado anteriormente, el nivel del riesgo se puede clasificar en una escala de 0 a 10, siendo el valor 0 el riesgo despreciable y el valor 10 el riesgo extremadamente crítico. Teniendo en cuenta dicha escala, y tomando como métrica para el nivel de riesgo el mayor valor de riesgo identificado en un activo, **el resultado del Análisis de Riesgos determina un Nivel de Riesgo Actual = {2,6}**.

Atendiendo a los niveles mínimos de madurez requeridos por el Esquema Nacional de Seguridad y tomando para el riesgo objetivo la misma métrica que se ha tomado para el riesgo residual, es decir, el mayor valor de riesgo identificado en un activo, el objetivo que se propone alcanzar en el proceso de mitigación de riesgos quedaría establecido en un **Nivel de Riesgo Objetivo = {1,8}**.

Activos	Riesgo Actual	Riesgo Objetivo
[001] Servicio Radar Covid19	2,6	1,8
[SP-0001] Soportes	1	1
[L-0001] Instalaciones AWS	0,9	0,9
[HW-0002] Equipos AWS	0,9	0,9
[SW-0001] App Radar Covid19	0,9	0,9
[COM-0001] Redes de Comunicaciones	0,9	0,9
[SS-0002] Servicio Cloud	0,8	0,8
[SE-0002] Repositorio Descargas (APPLE STORE)	0,8	0,8
[SE-0001] Repositorio Descargas (ANDROID STORE)	0,8	0,8
[P-0002] Administradores / Operadores	0,8	0,8
[SS-0001] Desarrollo y Mantenimiento de la App	0,8	0,8
[P-0003] Desarrolladores	0,6	0,6
[P-0001] Ciudadanos	0,5	0,5
[HW-0001] Teléfono Móvil	0,4	0,4
Total general	2,6	1,8

Tabla 9 Evolución de los Riesgos

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

Las acciones propuestas en este caso son:

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

Anexo I – Inventario de Activos

Inventario de Activos

INVENTARIO DE ACTIVOS		
TIPO	CÓDIGO	NOMBRE DE ACTIVO
[B] Activos esenciales		
	[001]	Servicio Radar Covid19
[E] Equipamiento		
[SW] Aplicaciones		
	[SW-0001]	App Radar Covid19
[HW] Equipos		
	[HW-0001]	Teléfono Móvil
	[HW-0002]	Equipos AWS
[COM] Comunicaciones		
	[COM-0001]	Redes de Comunicaciones
[SP] SOPORTES		
	[SP-0001]	Soportes
[SS] Servicios Subcontratados		
	[SS-0001]	Desarrollo y Mantenimiento de la App
	[SS-0002]	Servicio Cloud
[SE] Servicios Externos		
	[SE-0001]	Repositorio Descargas (ANDROID STORE)
	[SE-0002]	Repositorio Descargas (APPLE STORE)
[L] Instalaciones		
	[L-0001]	Instalaciones AWS
[P] Personal		
	[P-0001]	Ciudadanos
	[P-0002]	Administradores / Operadores
	[P-0003]	Desarrolladores

Tabla 10 Inventario de Activos

Clases de Activos

CLASES DE ACTIVOS			
TIPO	CÓDIGO	NOMBRE DE ACTIVO	CLASES
[B] Activos esenciales	[001]	Servicio Radar Covid19	{essential.{info.{adm,per.{pseudonymous,sensitive.7.5}},service},D.{files,e-files}}
[E] Equipamiento			
[SW] Aplicaciones			
	[SW-0001]	App Radar Covid19	{SW.sub}
[HW] Equipos			
	[HW-0001]	Teléfono Móvil	{HW.{mobile,iphone}}
	[HW-0002]	Equipos AWS	{HW.{host,vhost,backup,data}}
[COM] Comunicaciones			
	[COM-0001]	Redes de Comunicaciones	{arch.ip,HW.{network.{switch,router}},COM.{PSTN,wifi,mobile}}
[SP] SOPORTES			
	[SP-0001]	Soportes	{media.electronic}
[SS] Servicios Subcontratados			
	[SS-0001]	Desarrollo y Mantenimiento de la App	{S.3rd}
	[SS-0002]	Servicio Cloud	{S.3rd.cloud}
[SE] Servicios Externos			
	[SE-0001]	Repositorio Descargas (ANDROID STORE)	{S.3rd.hosting}
	[SE-0002]	Repositorio Descargas (APPLE STORE)	{S.3rd.hosting}
[L] Instalaciones			
	[L-0001]	Instalaciones AWS	{AUX.{power,ups,gen,ac,cabling,supply},L.{site,building}}
[P] Personal			
	[P-0001]	Ciudadanos	{p.ue}
	[P-0002]	Administradores / Operadores	{p.{op,adm,com,dba,sec}}
	[P-0003]	Desarrolladores	{p.{dev.prov}}

Tabla 11 Clases de Activos

Para el activo “*Servicio Radar Covid19*” se ha incorporado la siguiente información relativa al RGPD:

[001] A.1.1. identificación > activo > RGPD

activos

roles necesidad ciclo de vida necesidad y proporcionalidad

[001] Servicio Radar Covid19

DPD (Delegado de Protección de Datos)

Datos de la Entidad Razón Social: MINISTERIO DE SANIDAD Dirección: PASEO DEL PRADO, NUM 18, MADRID (28071, MADRID ESPAÑA NIF: S2827001E Datos de contacto del DPD: RECURSOS HUMANOS-INSPECCION@SANIDAD.GOB.ES PASEO DEL PRADO, NUM 18, MADRID (28071), MADRID - ESPAÑA NIF: S2827001E


Responsable del tratamiento

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

Encargado del tratamiento

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. Deben considerarse encargados del tratamiento los fabricantes de los sistemas operativos y de los dispositivos como responsables de la API que permite el tratamiento de datos personales por las aplicaciones de los dispositivos móviles. Así como todos los proveedores que intervengan y tengan o puedan tener acceso a los datos. En virtud de la 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, y por tanto en el supuesto de que tenga lugar un intercambio fronterizo de datos dentro de la UE, a través de la pasarela federativa entre las autoridades nacionales designadas o los organismos oficiales designados, la Comisión Europea actúa en calidad de encargado del tratamiento como proveedora de soluciones técnicas y organizativas de la citada pasarela federativa, y tratará los datos personales seudonimizados en nombre de los Estados miembros participantes como corresponsables en la pasarela federativa.

😊 ? 😞


[001] A.1.1. identificación > activo > RGPD

activos

roles

necesidad

ciclo de vida

necesidad y proporcionalidad

[001] Servicio Radar Covid19

Análisis de la necesidad de realizar una EIPD

1 Tipos de operaciones específicamente considerados por la Autoridad de control

¿El tratamiento a analizar se encuentra dentro de la lista de tipos de tratamientos de datos publicados por la AEPD que requieren una EIPD?

[] 1. Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.

[] 2. Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

[x] 3. 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.

[x] 4. Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

[] 5. Tratamientos que impliquen el uso de datos biométricos con el propósito de identificar de manera única a una persona física.

[] 6. Tratamientos que impliquen el uso de datos genéticos para cualquier fin.




[x] 7. 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.

[] 8. Tratamientos que impliquen la asociación, combinación o enlace de registros de bases de datos de dos o más tratamientos con finalidades diferentes o por responsables distintos.

[] 9. Tratamientos de datos de sujetos vulnerables o en riesgo de exclusión social, incluyendo datos de menores de 14 años, mayores con algún grado de discapacidad, discapacitados, personas que acceden a servicios sociales y víctimas de violencia de género, así como sus descendientes y personas que estén bajo su guardia y custodia.

[x] 10. 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.

[] 11. Tratamientos de datos que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato, como por ejemplo tratamientos en los que los datos han sido recopilados por un responsable distinto al que los va a tratar y aplica alguna de las excepciones sobre la información que debe proporcionarse a los interesados según el artículo 14.5 (b,c,d) del RGPD.

Análisis de riesgos

26

P [001] A.1.1. identificación > activo > RGPD

activos

roles | necesidad | **ciclo de vida** | necesidad y proporcionalidad

[001] Servicio Radar Covid19

Ciclo de vida de los datos

1 Captura de datos

Actividades del proceso

Acceso a información almacenada en el dispositivo móvil en el momento de la instalación de la App.

Datos tratados

Datos que el usuario tenga instalados en su dispositivo móvil. Información almacenada en el dispositivo móvil en el momento de la instalación de la App.

Intervinientes involucrados

usuarios

Tecnologías intervinientes

Dispositivo móvil

2 Clasificación / Almacenamiento

Actividades del proceso

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 solo entre terminales móviles. 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.

Datos tratados

Códigos aleatorios: Se generan en el back-end del sistema. Códigos anónimos de otros usuarios que también tienen instalada la App. Balizas de los usuarios que hayan sido diagnosticados de Covid-19.

Intervinientes involucrados

Administradores de Amazon

Tecnologías intervinientes

Servidor externo: Servidor de Amazon.

⬅ ||| ➡

😊 ? 😞

P [001] A.1.1. identificación > activo > RGPD

activos

roles necesidad **ciclo de vida** necesidad y proporcionalidad

[001] Servicio Radar Covid19

3 Uso / Tratamiento

Actividades del proceso

Las autoridades sanitarias entregan el código de positivo a un usuario con PCR positiva que lo introduce en el dispositivo móvil. 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.

Datos tratados

Código de positivo.

Intervinientes involucrados

Autoridades sanitarias Usuarios

Tecnologías intervinientes

Servicios Autonómicos de Salud y servidores de AWS.

4 Cesión o transferencia de los datos a un tercero para su tratamiento

Actividades del proceso

Integración con otros sistemas de la Unión Europea (no hay transferencia internacional de datos).

Datos tratados

Códigos aleatorios generados. Códigos anónimos de otros usuarios que también tienen instalada la App. Balizas de los usuarios que hayan sido diagnosticados de Covid-19.

Intervinientes involucrados

Comisión Europea.

Tecnologías intervinientes

Pasarela Federativa.

😊 ? 😞

P [001] A.1.1. identificación > activo > RGPD

activos

roles necesidad **ciclo de vida** necesidad y proporcionalidad

[001] Servicio Radar Covid19

5 Destrucción

Actividades del proceso

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 servidores).

Datos tratados

Códigos aleatorios generados. Códigos anónimos de otros usuarios que también tienen instalada la App. Balizas de los usuarios que hayan sido diagnosticados de Covid-19. Código de positivo.


Intervinientes involucrados

Usuarios. Administradores de Amazon. Autoridades sanitarias.

Tecnologías intervinientes

Desinstalación de la Aplicación. Datos en servidores de Amazon y datos en servidor central.

😊 ? 😞

 [001] A.1.1. identificación > activo > RGPD

activos

roles

necesidad

ciclo de vida

necesidad y proporcionalidad

[001] Servicio Radar Covid19

Análisis de la necesidad y proporcionalidad del tratamiento

1 Legitimación

☒ Consentimiento

☐ Relación contractual

☒ Intereses vitales del interesado o de otras personas

☐ Obligación legal del responsable




☒ Interés público o ejercicio de poderes públicos


☒ Intereses legítimos prevalentes del responsable o de terceros

Legitimación

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

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


[001] A.1.1. identificación > activo > RGPD

activos

roles




necesidad

ciclo de vida

necesidad y proporcionalidad

[001] Servicio Radar Covid19

fin, incluso aunque se dirijan a proteger personas inominadas 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 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 salvaguarda 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 el 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 responsables de tratamientos de datos personales, cuando, por indicación de las autoridades sanitarias competentes, es necesario comunicar a otras personas con la 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

P [001] A.1.1. identificación > activo > RGPD

activos

roles necesidad ciclo de vida **necesidad y proporcionalidad**

[001] Servicio Radar Covid19

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 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 Ministerio 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 II 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 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.

III

😊 ? 😞

P [001] A.1.1. identificación > activo > RGPD

activos

roles necesidad ciclo de vida **necesidad y proporcionalidad**

[001] Servicio Radar Covid19

2 Evaluación del interés legítimo (cumplimentar si anteriormente se ha seleccionado 'Interés legítimo')

[] ¿El tratamiento es conforme a la legislación nacional y de la UE?

¿Existe la posibilidad de que algún aspecto del tratamiento a realizar entre en conflicto con alguna Ley de la UE? En tal caso, detallarlo

[] ¿El tratamiento representa un interés real y actual de la entidad?

Los intereses de la empresa no pueden prevalecer sobre los de los interesado. La finalidad del tratamiento debe verse amparada bajo legitimación.

[] ¿Existen otros medios menos invasivos para alcanzar la finalidad prevista del tratamiento y satisfacer el interés legítimo del responsable del tratamiento?

Debe adoptarse la vía en la que la intimidad del interesado, así como la de sus datos, se vea menos afectada.

[] ¿Cuál es la naturaleza del interés de la entidad?

Describir detalladamente la razón y alcance del tratamiento que se va a hacer de los datos del interesado.

[] ¿Cuál es el perjuicio que el responsable del tratamiento, los terceros o la comunidad en general puedan sufrir si no se realiza el tratamiento de datos?

Detallar las acciones o consecuencias que puede acarrear al responsable del tratamiento la no realización del tratamiento de datos.

[] ¿Existe un desequilibrio entre la situación del interesado y la del responsable del tratamiento?


Ejemplos de personas que pueden considerarse vulnerables: menores, personas mayores, discapacitados, refugiados y/o solicitantes de asilo, etc.

[x] ¿El interesado ha sido debidamente informado sobre las actividades del tratamiento?

Se debe informar de las acciones, labores y tareas que se van a llevar a cabo con los datos del interesado, así como el alcance de las mismas.

III

😊 ? 😞


[001] A.1.1. identificación > activo > RGPD

activos

roles

necesidad

ciclo de vida

necesidad y proporcionalidad




[001] Servicio Radar Covid19

[] ¿Qué perjuicios pueden ocasionarse al interesado?

Habrà 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 o 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, reidentificación por localización implícita, de la fragilidad de los protocolos a la hora de 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 del 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.

[] ¿Se trata de un tratamiento normalizado en el sector?

No.

P [001] A.1.1. identificación > activo > RGPD

activos

roles necesidad ciclo de vida **necesidad y proporcionalidad**

[001] Servicio Radar Covid19




3 Evaluación de la necesidad y proporcionalidad de las operaciones de Tratamiento

[x] Los datos recogidos se van a usar exclusivamente para la finalidad declarada y no para ninguna otra no informada ni incompatible con la legitimidad de su uso (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 informales 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 contiene 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 decide 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 debería 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.

[x] La finalidad que se pretende cubrir requiere de todos los datos a recabar y para todas las personas/interesados afectados (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 ofrezca consejos relacionados, por ejemplo, con la duración de la auto cuarentena.



Dependencias entre Activos

DEPENDENCIAS ENTRE ACTIVOS	
ACTIVOS	DEPENDENCIAS
[001] Servicio Radar Covid19	[SW-0001] App Radar Covid19
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[SS-0001] Desarrollo y Mantenimiento de la App
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
	[SS-0002] Servicio Cloud
	[HW-0002] Equipos AWS
	[L-0001] Instalaciones AWS
	[COM-0001] Redes de Comunicaciones
	[P-0002] Administradores / Operadores
	[SP-0001] Soportes
	[L-0001] Instalaciones AWS
	[SE-0001] Repositorio Descargas (ANDROID STORE)
	[SE-0002] Repositorio Descargas (APPLE STORE)
[SW] Aplicaciones	
[SW-0001] App Radar Covid19	
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[SS-0001] Desarrollo y Mantenimiento de la App
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
	[SS-0002] Servicio Cloud
	[HW-0002] Equipos AWS
	[L-0001] Instalaciones AWS
[HW] Equipos	
[HW-0001] Teléfono Móvil	
	[P-0001] Ciudadanos
[HW-0002] Equipos AWS	
	[L-0001] Instalaciones AWS
[COM] Comunicaciones	
[COM-0001] Redes de Comunicaciones	
	[P-0002] Administradores / Operadores
[SP] SOPORTES	
[SP-0001] Soportes	
	[L-0001] Instalaciones AWS
[SS-0001] Desarrollo y Mantenimiento de la App	
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[SS-0002] Servicio Cloud	
	[HW-0002] Equipos AWS
	[L-0001] Instalaciones AWS
[SE-0001] Repositorio Descargas (ANDROID STORE)	
[SE-0002] Repositorio Descargas (APPLE STORE)	
[L-0001] Instalaciones AWS	
[P-0001] Ciudadanos	
[P-0002] Administradores / Operadores	
[P-0003] Desarrolladores	

Tabla 12 Dependencias entre Activos

Valoración del Servicio Radar Covid19

Debido a la tipología de datos que trata el **servicio Radar Covid19** y a lo indicado en la Guía CCN-STIC 803, la valoración en cada una de las dimensiones de seguridad (Autenticidad, Confidencialidad, Integridad, Disponibilidad y Trazabilidad) debería ser al menos MEDIO, sin embargo, debido a la situación política y socioeconómica en la que nos encontramos originada por la pandemia Covid 19 y al impacto que supondría una brecha de seguridad de la información que trata, el **Servicio Radar Covid19** ha sido evaluado con una **categoría ALTA**. A continuación se indican las valoraciones que se ha dado en cada una de las dimensiones de seguridad:

- **AUTENTICIDAD:** Entendemos que, por la situación política y socioeconómica en la que nos encontramos debido a la pandemia, el impacto que tendría una pérdida de autenticidad de la información que trata la aplicación supondría:
 - Daño reputacional grave con los ciudadanos o con otras organizaciones
 - Protestas masivas (alteración sería del orden público)

La Guía de Seguridad CCN-STIC 803 determina que ante consecuencias de este tipo es necesario considerar un **nivel ALTO**.

- **CONFIDENCIALIDAD:** Entendemos que, por la situación política y socioeconómica en la que nos encontramos debido a la pandemia, el impacto que tendría una pérdida de confidencialidad en la información que trata la aplicación supondría:
 - Daño reputacional grave con los ciudadanos o con otras organizaciones
 - Protestas masivas (alteración sería del orden público)

La Guía de Seguridad CCN-STIC 803 determina que ante consecuencias de este tipo es necesario considerar un **nivel ALTO**.

- **INTEGRIDAD:** Entendemos que, por la situación política y socioeconómica en la que nos encontramos debido a la pandemia, el impacto que tendría una pérdida de integridad supondría:
 - Daño reputacional grave con los ciudadanos o con otras organizaciones
 - Protestas masivas (alteración sería del orden público)

La Guía de Seguridad CCN-STIC 803 determina que ante consecuencias de este tipo es necesario considerar un **nivel ALTO**.

- **DISPONIBILIDAD:** La Guía CCN-STIC 803, dependiendo del plazo necesario para restaurar los niveles mínimos de servicio la aplicación propone el nivel de seguridad que debería asignarse a la Disponibilidad. En este caso entendemos que el servicio debería restaurarse en un plazo máximo de 4 horas y por tanto se propone que la Disponibilidad tenga **nivel ALTO**.

- **TRAZABILIDAD:** Entendemos que, por la situación política y socioeconómica en la que nos encontramos debido a la pandemia, el impacto que tendría no poder comprobar a posteriori quien ha accedido a, o modificado, una cierta información supondría:
 - Daño reputacional grave con los ciudadanos o con otras organizaciones
 - Protestas masivas (alteración sería del orden público)

La Guía de Seguridad CCN-STIC 803 determina que ante consecuencias de este tipo es necesario considerar un **nivel ALTO**.

- **DATOS PERSONALES:** Entendemos que, por la situación política y socioeconómica en la que nos encontramos debido a la pandemia, y teniendo en cuenta que el Servicio Radar Covid19 tiene datos categorizados como sensibles, es necesario considerar un **nivel ALTO**.

VALORACIÓN DE ACTIVOS							
ACTIVOS	A	C	I	D	A	DP	VALORACIÓN
[0001] Servicio Radar Covid19	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO
	ALTO	ALTO	ALTO	ALTO	ALTO	ALTO	

Tabla 13 Valoración de Activos

Anexo II – Criterios de Valoración de las Dimensiones de Seguridad

El presente anexo describe los criterios de valoración aplicados para cada dimensión de seguridad valorada:

DIMENSIONES	El Nivel de Seguridad se establecerá en función de las consecuencias que tendría ...	Impacto ¿Qué pasa si ...?
Autenticidad [A]	... el hecho de que la información no fuera auténtica.	¿Qué pasa si no puedo garantizar la identidad del origen y/o destino de la información?
Confidencialidad [C]	... su revelación a personas no autorizadas o que no necesitan conocer la información.	¿Qué sucede si la información cae en manos de terceros?
Integridad [I]	... su modificación por alguien que no está autorizado a modificar la información.	¿Qué impacto tendría que la información sea modificada por alguien no autorizado?
Disponibilidad [D]	... el que una persona autorizada no pudiera acceder a la información cuando la necesita.	¿Qué pasa si la información deja de estar disponible en el lugar, forma y momento requeridos?
Auditabilidad [A] o Trazabilidad	... el no poder rastrear a posteriori quién ha accedido a o modificado una cierta información.	¿Qué conlleva que el tratamiento de la información (acceso, modificación, borrado) no pueda ser verificado (trazado)?

CRITERIOS DE VALORACIÓN				
DIMENSIONES	NIVEL ALTO	NIVEL MEDIO	NIVEL BAJO	SIN VALORAR
Autenticidad [A]	La falsedad en el origen y destino causaría daños muy graves, irreparables .	La falsedad en el origen y destino causaría daños significativos y de difícil reparación .	La falsedad en el origen y destino causaría perjuicio limitado , pudiendo ser subsanable	La falsedad en el origen y destino es irrelevante (anonimato).
Confidencialidad [C]	Debe ser conocida solo por un número muy reducido de personas . Su revelación causaría daños de difícil o imposible reparación, perjuicios muy graves de imagen, legales, económicos, etc.	Solo debe ser conocida por las personas que la necesitan para su trabajo, con autorización explícita . Su revelación causaría daños importantes aunque subsanables, perjuicios graves de imagen, legales, económicos, etc.	No debe ser conocida por personas ajenas a la organización . Su revelación causaría algún perjuicio leve de imagen, legal, etc.	Información de carácter público o cuya revelación no causa perjuicio alguno.
Integridad [I]	Su manipulación o modificación no autorizada causaría un daño muy grave de imposible o muy difícil recuperación .	Su manipulación o modificación no autorizada causaría un perjuicio grave, aunque subsanable (acciones correctoras costosas).	Su manipulación o modificación no autorizada causaría algún inconveniente (incumplimiento leve de una norma, retrasos leves o modificación de los resultados con poca repercusión).	Errores en la información o en el servicio carecen de consecuencias .

CRITERIOS DE VALORACIÓN				
DIMENSIONES	NIVEL ALTO	NIVEL MEDIO	NIVEL BAJO	SIN VALORAR
Disponibilidad [D]	Si la información o el servicio no están disponibles en menos de 4 horas , el daño causado es muy grave .	Si la información o el servicio no están disponibles durante más de 1 día , el perjuicio es grave y de costosa reparación .	Se puede prescindir hasta 5 días , a partir de los cuales se causa un perjuicio limitado , pero subsanable.	Se puede prescindir de la información o el servicio durante más de 5 días sin que ello provoque un perjuicio relevante.
Trazabilidad [T]	La incapacidad de rastrear un acceso a la información ocasionaría un perjuicio muy grave , de difícil o imposible reparación o la incapacidad para perseguir delitos .	La incapacidad de rastrear un acceso a la información dificultaría la subsanación de problemas , provocando un perjuicio grave o dificultaría gravemente la capacidad para perseguir delitos .	La pérdida de trazabilidad dificultaría la subsanación de problemas , causando un perjuicio limitado .	Es irrelevante conocer la autoría de las actuaciones sobre la información o el servicio.

Tabla 14 Criterios de Valoración de las Dimensiones de Seguridad

Anexo III – Caracterización de Salvaguardas

Madurez ENS

La siguiente tabla contiene el grado de madurez de las medidas de seguridad del ENS que han sido cargadas en la Herramienta PILAR:

REF.	MEDIDAS	ESQUEMA NACIONAL DE SEGURIDAD	CMM
org	MARCO ORGANIZATIVO		
	org.1	Política de seguridad	L4
	org.2	Normativa de seguridad	L4
	org.3	Procedimientos de seguridad	L4
	org.4	Proceso de autorización	L3
op	MARCO OPERACIONAL		
op.pl	Planificación		
	op.pl.1	Análisis de riesgos	L4
	op.pl.2	Arquitectura de seguridad	L3
	op.pl.3	Adquisición de nuevos componentes	L3
	op.pl.4	Dimensionamiento / gestión de capacidades	L3
	op.pl.5	Componentes certificados	L2
op.acc	Control de acceso		
	op.acc.1	Identificación	L3
	op.acc.2	Requisitos de acceso	L3
	op.acc.3	Segregación de funciones y tareas	L3
	op.acc.4	Proceso de gestión de derechos de acceso	L3
	op.acc.5	Mecanismo de autenticación	L2
	op.acc.6	Acceso local (Local Logon)	L2
	op.acc.7	Acceso remoto (Remote Login)	L2
op.exp	Explotación		
	op.exp.1	Inventario de activos	L4
	op.exp.2	Configuración de seguridad	L4
	op.exp.3	Gestión de la configuración	L4
	op.exp.4	Mantenimiento	L3
	op.exp.5	Gestión de cambios	L4
	op.exp.6	Protección frente a código dañino	L4
	op.exp.7	Gestión de incidentes	L4
	op.exp.8	Registro de la actividad de los usuarios	L3

	op.exp.9	Registro de la gestión de incidentes	L3
	op.exp.10	Protección de los registros de actividad	L3
	op.exp.11	Protección de claves criptográficas	L4
op.ext	Servicios externos		
	op.ext.1	Contratación y acuerdos de nivel de servicio	L2
	op.ext.2	Gestión diaria	L2
	op.ext.9	Medios alternativos	L3
op.cont	Continuidad del servicio		
	op.cont.1	Análisis de impacto	L4
	op.cont.2	Plan de continuidad	L3
	op.cont.3	Pruebas periódicas	L3
op.mon	Monitorización del sistema		
	op.mon.1	Detección de intrusión	L3
	op.mon.2	Sistema de métricas	L2
mp	MEDIDAS DE PROTECCIÓN		
mp.if	Protección de las instalaciones e infraestructuras		
	mp.if.1	Áreas separadas y con control de acceso	L3
	mp.if.2	Identificación de las personas	L3
	mp.if.3	Acondicionamiento de los locales	L3
	mp.if.4	Energía eléctrica	L3
	mp.if.5	Protección frente a incendios	L3
	mp.if.6	Protección frente a inundaciones	L3
	mp.if.7	Registro de entrada y salida de equipamiento	L3
	mp.if.9	Instalaciones alternativas	L4
mp.per	Gestión del personal		
	mp.per.1	Caracterización del puesto de trabajo	L4
	mp.per.2	Deberes y obligaciones	L4
	mp.per.3	Concienciación	L3
	mp.per.4	Formación	L4
	mp.per.9	Personal alternativo	L3
mp.eq	Protección de los equipos		
	mp.eq.1	Puesto de trabajo despejado	L3
	mp.eq.2	Bloqueo de puesto de trabajo	L4
	mp.eq.3	Protección de portátiles	L3
	mp.eq.9	Medios alternativos	L4

mp.com	Protección de las comunicaciones		
	mp.com.1	Perímetro seguro	L3
	mp.com.2	Protección de la confidencialidad	L3
	mp.com.3	Protección de la autenticidad y de la integridad	L3
	mp.com.4	Segregación de redes	L4
	mp.com.9	Medios alternativos	L4
mp.si	Protección de los soportes de información		
	mp.si.1	Etiquetado	L4
	mp.si.2	Criptografía	L4
	mp.si.3	Custodia	L4
	mp.si.4	Transporte	L4
	mp.si.5	Borrado y destrucción	L4
mp.sw	Protección de las aplicaciones informáticas		
	mp.sw.1	Desarrollo de aplicaciones	L3
	mp.sw.2	Aceptación y puesta en servicio	L4
mp.info	Protección de la información		
	mp.info.1	Datos de carácter personal	L5
	mp.info.2	Calificación de la información	L2
	mp.info.3	Cifrado de la información	L5
	mp.info.4	Firma electrónica	L2
	mp.info.5	Sellos de tiempo	N/A
	mp.info.6	Limpieza de documentos	L3
	mp.info.9	Copias de seguridad	L3
mp.s	Protección de los servicios		
	mp.s.1	Protección del correo electrónico (e-mail)	L4
	mp.s.2	Protección de servicios y aplicaciones web	L3
	mp.s.8	Protección frente a la denegación de servicio	L4
	mp.s.9	Medios alternativos	L4

Tabla 15 Caracterización de las Salvaguardas ENS

Madurez RGPD

La siguiente tabla contiene el grado de madurez de los artículos del RGPD que han sido cargados en la Herramienta PILAR:

ARTÍCULO RGPD	CMM
Artículo 5 - Principios relativos al tratamiento	
1. Los datos personales serán:	
a) tratados de manera lícita, leal y transparente en relación con el interesado («licitud, lealtad y transparencia»);	90%
b) recogidos con fines determinados, explícitos y legítimos, y no serán tratados ulteriormente de manera incompatible con dichos fines; de acuerdo con el artículo 89, apartado 1, el tratamiento ulterior de los datos personales con fines de archivo en interés público, fines de investigación científica e histórica o fines estadísticos no se considerará incompatible con los fines iniciales («limitación de la finalidad»);	90%
c) adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados («minimización de datos»);	90%
d) exactos y, si fuera necesario, actualizados; se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan («exactitud»);	80%
e) mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales; los datos personales podrán conservarse durante periodos más largos siempre que se traten exclusivamente con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sin perjuicio de la aplicación de las medidas técnicas y organizativas apropiadas que impone el presente Reglamento a fin de proteger los derechos y libertades del interesado («limitación del plazo de conservación»);	90%
f) tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas («integridad y confidencialidad»).	80%
2. El responsable del tratamiento será responsable del cumplimiento de lo dispuesto en el apartado 1 y capaz de demostrarlo («responsabilidad proactiva»).	90%
Artículo 6 - Licitud del tratamiento	
1. El tratamiento solo será lícito si se cumple al menos una de las siguientes condiciones:	
a) el interesado dio su consentimiento para el tratamiento de sus datos personales para uno o varios fines específicos;	100%
b) el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales;	N/A
c) el tratamiento es necesario para el cumplimiento de una obligación legal aplicable al responsable del tratamiento;	100%
d) el tratamiento es necesario para proteger intereses vitales del interesado o de otra persona física;	100%
e) el tratamiento es necesario para el cumplimiento de una misión realizada en interés público o en el ejercicio de poderes públicos conferidos al responsable del tratamiento;	100%
f) el tratamiento es necesario para la satisfacción de intereses legítimos perseguidos por el responsable del tratamiento o por un tercero, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos y libertades fundamentales del interesado que requieran la protección de datos personales, en particular cuando el interesado sea un niño.	N/A
4. Cuando el tratamiento para otro fin distinto de aquel para el que se recogieron los datos personales no esté basado en el consentimiento del interesado o en el Derecho de la Unión o de los Estados miembros que constituya una medida necesaria y proporcional en una sociedad democrática para salvaguardar los objetivos indicados en el artículo 23, apartado 1, el responsable del tratamiento, con objeto de determinar si el tratamiento con otro fin es compatible con el fin para el cual se recogieron inicialmente los datos personales, tendrá en cuenta, entre otras cosas:	
a) cualquier relación entre los fines para los cuales se hayan recogido los datos personales y los fines del tratamiento ulterior previsto;	N/A

ARTÍCULO RGPD		CMM
b) el contexto en que se hayan recogido los datos personales, en particular por lo que respecta a la relación entre los interesados y el responsable del tratamiento;		N/A
c) la naturaleza de los datos personales, en concreto cuando se traten categorías especiales de datos personales, de conformidad con el artículo 9, o datos personales relativos a condenas e infracciones penales, de conformidad con el artículo 10;		N/A
d) las posibles consecuencias para los interesados del tratamiento ulterior previsto;		N/A
e) la existencia de garantías adecuadas, que podrán incluir el cifrado o la seudonimización.		N/A
Artículo 7 - Condiciones para el consentimiento		
1. Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de demostrar que aquel consintió el tratamiento de sus datos personales.		90%
2. Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se presentará de tal forma que se distinga claramente de los demás asuntos, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo. No será vinculante ninguna parte de la declaración que constituya infracción del presente Reglamento.		90%
3. El interesado tendrá derecho a retirar su consentimiento en cualquier momento. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.		90%
4. Al evaluar si el consentimiento se ha dado libremente, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, se supedita al consentimiento al tratamiento de datos personales que no son necesarios para la ejecución de dicho contrato.		100%
Artículo 8 - Condiciones aplicables al consentimiento del niño en relación con los servicios de la sociedad de la información		
1. Cuando se aplique el artículo 6, apartado 1, letra a), en relación con la oferta directa a niños de servicios de la sociedad de la información, el tratamiento de los datos personales de un niño se considerará lícito cuando tenga como mínimo 16 años. Si el niño es menor de 16 años, tal tratamiento únicamente se considerará lícito si el consentimiento lo dio o autorizó el titular de la patria potestad o tutela sobre el niño, y solo en la medida en que se dio o autorizó.		N/A
2. El responsable del tratamiento hará esfuerzos razonables para verificar en tales casos que el consentimiento fue dado o autorizado por el titular de la patria potestad o tutela sobre el niño, teniendo en cuenta la tecnología disponible.		N/A
Artículo 9 - Tratamiento de categorías especiales de datos personales		
2. El apartado 1 no será de aplicación cuando concorra una de las circunstancias siguientes:		
a) el interesado dio su consentimiento explícito para el tratamiento de dichos datos personales con uno o más de los fines especificados, excepto cuando el Derecho de la Unión o de los Estados miembros establezca que la prohibición mencionada en el apartado 1 no puede ser levantada por el interesado;		80%
b) el tratamiento es necesario para el cumplimiento de obligaciones y el ejercicio de derechos específicos del responsable del tratamiento o del interesado en el ámbito del Derecho laboral y de la seguridad y protección social, en la medida en que así lo autorice el Derecho de la Unión de los Estados miembros o un convenio colectivo con arreglo al Derecho de los Estados miembros que establezca garantías adecuadas del respeto de los derechos fundamentales y de los intereses del interesado;		N/A
c) 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;		N/A
d) el tratamiento es efectuado, en el ámbito de sus actividades legítimas y con las debidas garantías, por una fundación, una asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que el tratamiento se refiera exclusivamente a los miembros actuales o antiguos de tales organismos o a personas que		N/A

ARTÍCULO RGPD	CMM
mantengan contactos regulares con ellos en relación con sus fines y siempre que los datos personales no se comuniquen fuera de ellos sin el consentimiento de los interesados;	
e) el tratamiento se refiere a datos personales que el interesado ha hecho manifiestamente públicos;	N/A
f) el tratamiento es necesario para la formulación, el ejercicio o la defensa de reclamaciones o cuando los tribunales actúen en ejercicio de su función judicial;	N/A
g) el tratamiento es necesario por razones de un interés público esencial, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado;	100%
h) el tratamiento es necesario para fines de medicina preventiva o laboral, evaluación de la capacidad laboral del trabajador, diagnóstico médico, prestación de asistencia o tratamiento de tipo sanitario o social, o gestión de los sistemas y servicios de asistencia sanitaria y social, sobre la base del Derecho de la Unión o de los Estados miembros o en virtud de un contrato con un profesional sanitario y sin perjuicio de las condiciones y garantías contempladas en el apartado 3;	N/A
i) el tratamiento es necesario por razones de interés público en el ámbito de la salud pública, como la protección frente a amenazas transfronterizas graves para la salud, o para garantizar elevados niveles de calidad y de seguridad de la asistencia sanitaria y de los medicamentos o productos sanitarios, 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,	100%
j) el tratamiento es necesario con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, de conformidad con el artículo 89, apartado 1, sobre la base del Derecho de la Unión o de los Estados miembros, que debe ser proporcional al objetivo perseguido, respetar en lo esencial el derecho a la protección de datos y establecer medidas adecuadas y específicas para proteger los intereses y derechos fundamentales del interesado.	100%
3. Los datos personales a que se refiere el apartado 1 podrán tratarse a los fines citados en el apartado 2, letra h), cuando su tratamiento sea realizado por un profesional sujeto a la obligación de secreto profesional, o bajo su responsabilidad, de acuerdo con el Derecho de la Unión o de los Estados miembros o con las normas establecidas por los organismos nacionales competentes, o por cualquier otra persona sujeta también a la obligación de secreto de acuerdo con el Derecho de la Unión o de los Estados miembros o de las normas establecidas por los organismos nacionales competentes.	N/A
Artículo 10 - Tratamiento de datos personales relativos a condenas e infracciones penales	
El tratamiento de datos personales relativos a condenas e infracciones penales o medidas de seguridad conexas sobre la base del artículo 6, apartado 1, sólo podrá llevarse a cabo bajo la supervisión de las autoridades públicas o cuando lo autorice el Derecho de la Unión o de los Estados miembros que establezca garantías adecuadas para los derechos y libertades de los interesados. Solo podrá llevarse un registro completo de condenas penales bajo el control de las autoridades públicas.	N/A
Artículo 11 - Tratamiento que no requiere identificación	
2. Cuando, en los casos a que se refiere el apartado 1 del presente artículo, el responsable sea capaz de demostrar que no está en condiciones de identificar al interesado, le informará en consecuencia, de ser posible. En tales casos no se aplicarán los artículos 15 a 20, excepto cuando el interesado, a efectos del ejercicio de sus derechos en virtud de dichos artículos, facilite información adicional que permita su identificación.	N/A
Artículo 12 - Transparencia de la información, comunicación y modalidades de ejercicio de los derechos del interesado	
C52:D58cada en los artículos 13 y 14, así como cualquier comunicación con arreglo a los artículos 15 a 22 y 34 relativa al tratamiento, en forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo, en particular cualquier información dirigida específicamente a un niño. La información será facilitada por escrito o por otros medios, inclusive, si procede, por medios electrónicos. Cuando lo solicite el interesado, la información	80%

ARTÍCULO RGPD		CMM
podrá facilitarse verbalmente siempre que se demuestre la identidad del interesado por otros medios.		
2. El responsable del tratamiento facilitará al interesado el ejercicio de sus derechos en virtud de los artículos 15 a 22. En los casos a que se refiere el artículo 11, apartado 2, el responsable no se negará a actuar a petición del interesado con el fin de ejercer sus derechos en virtud de los artículos 15 a 22, salvo que pueda demostrar que no está en condiciones de identificar al interesado.		N/A
3. El responsable del tratamiento facilitará al interesado información relativa a sus actuaciones sobre la base de una solicitud con arreglo a los artículos 15 a 22, y, en cualquier caso, en el plazo de un mes a partir de la recepción de la solicitud. Dicho plazo podrá prorrogarse otros dos meses en caso necesario, teniendo en cuenta la complejidad y el número de solicitudes. El responsable informará al interesado de cualquiera de dichas prórrogas en el plazo de un mes a partir de la recepción de la solicitud, indicando los motivos de la dilación. Cuando el interesado presente la solicitud por medios electrónicos, la información se facilitará por medios electrónicos cuando sea posible, a menos que el interesado solicite que se facilite de otro modo.		N/A
4. Si el responsable del tratamiento no da curso a la solicitud del interesado, le informará sin dilación, y a más tardar transcurrido un mes de la recepción de la solicitud, de las razones de su no actuación y de la posibilidad de presentar una reclamación ante una autoridad de control y de ejercitar acciones judiciales.		N/A
5. La información facilitada en virtud de los artículos 13 y 14 así como toda comunicación y cualquier actuación realizada en virtud de los artículos 15 a 22 y 34 serán a título gratuito. Cuando las solicitudes sean manifiestamente infundadas o excesivas, especialmente debido a su carácter repetitivo, el responsable del tratamiento podrá:		N/A
6. Sin perjuicio de lo dispuesto en el artículo 11, cuando el responsable del tratamiento tenga dudas razonables en relación con la identidad de la persona física que cursa la solicitud a que se refieren los artículos 15 a 21, podrá solicitar que se facilite la información adicional necesaria para confirmar la identidad del interesado.		N/A
7. La información que deberá facilitarse a los interesados en virtud de los artículos 13 y 14 podrá transmitirse en combinación con iconos normalizados que permitan proporcionar de forma fácilmente visible, inteligible y claramente legible una adecuada visión de conjunto del tratamiento previsto. Los iconos que se presenten en formato electrónico serán legibles mecánicamente.		80%
Artículo 13 - Información que deberá facilitarse cuando los datos personales se obtengan del interesado		
1. Cuando se obtengan de un interesado datos personales relativos a él, el responsable del tratamiento, en el momento en que estos se obtengan, le facilitará toda la información indicada a continuación:		
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;		50%
b) los datos de contacto del delegado de protección de datos, en su caso;		50%
c) los fines del tratamiento a que se destinan los datos personales y la base jurídica del tratamiento;		100%
d) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable o de un tercero;		N/A
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;		80%
f) en su caso, la intención del responsable de transferir datos personales a un tercer país u organización internacional y la existencia o ausencia de una decisión de adecuación de la Comisión, o, en el caso de las transferencias indicadas en los artículos 46 o 47 o el artículo 49, apartado 1, párrafo segundo, referencia a las garantías adecuadas o apropiadas y a los medios para obtener una copia de estas o al hecho de que se hayan prestado.		N/A
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado, en el momento en que se obtengan los datos personales, la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente:		

ARTÍCULO RGPD	CMM
a) el plazo durante el cual se conservarán los datos personales o, cuando no sea posible, los criterios utilizados para determinar este plazo;	80%
b) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, o a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;	N/A
c) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basado en el consentimiento previo a su retirada;	100%
d) el derecho a presentar una reclamación ante una autoridad de control;	100%
e) si la comunicación de datos personales es un requisito legal o contractual, o un requisito necesario para suscribir un contrato, y si el interesado está obligado a facilitar los datos personales y está informado de las posibles consecuencias de que no facilitar tales datos;	N/A
f) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.	N/A
3. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de datos personales para un fin que no sea aquel para el que se recogieron, proporcionará al interesado, con anterioridad a dicho tratamiento ulterior, información sobre ese otro fin y cualquier información adicional pertinente a tenor del apartado 2.	N/A
Artículo 14 - Información que deberá facilitarse cuando los datos personales no se hayan obtenido del interesado	
1. Cuando los datos personales no se hayan obtenidos del interesado, el responsable del tratamiento le facilitará la siguiente información:	
a) la identidad y los datos de contacto del responsable y, en su caso, de su representante;	N/A
b) los datos de contacto del delegado de protección de datos, en su caso;	N/A
c) los fines del tratamiento a que se destinan los datos personales, así como la base jurídica del tratamiento;	N/A
d) las categorías de datos personales de que se trate;	N/A
e) los destinatarios o las categorías de destinatarios de los datos personales, en su caso;	N/A
2. Además de la información mencionada en el apartado 1, el responsable del tratamiento facilitará al interesado la siguiente información necesaria para garantizar un tratamiento de datos leal y transparente respecto del interesado:	
a) el plazo durante el cual se conservarán los datos personales o, cuando eso no sea posible, los criterios utilizados para determinar este plazo;	N/A
b) cuando el tratamiento se base en el artículo 6, apartado 1, letra f), los intereses legítimos del responsable del tratamiento o de un tercero;	N/A
c) la existencia del derecho a solicitar al responsable del tratamiento el acceso a los datos personales relativos al interesado, y su rectificación o supresión, o la limitación de su tratamiento, y a oponerse al tratamiento, así como el derecho a la portabilidad de los datos;	N/A
d) cuando el tratamiento esté basado en el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), la existencia del derecho a retirar el consentimiento en cualquier momento, sin que ello afecte a la licitud del tratamiento basada en el consentimiento antes de su retirada;	N/A
e) el derecho a presentar una reclamación ante una autoridad de control;	N/A
f) la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público;	N/A
g) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.	N/A

ARTÍCULO RGPD	CMM
3. El responsable del tratamiento facilitará la información indicada en los apartados 1 y 2:	
a) dentro de un plazo razonable, una vez obtenidos los datos personales, y a más tardar dentro de un mes, habida cuenta de las circunstancias específicas en las que se traten dichos datos;	N/A
b) si los datos personales han de utilizarse para comunicación con el interesado, a más tardar en el momento de la primera comunicación a dicho interesado, o	N/A
c) si está previsto comunicarlos a otro destinatario, a más tardar en el momento en que los datos personales sean comunicados por primera vez.	N/A
4. Cuando el responsable del tratamiento proyecte el tratamiento ulterior de los datos personales para un fin que no sea aquel para el que se obtuvieron, proporcionará al interesado, antes de dicho tratamiento ulterior, información sobre ese otro fin y cualquier otra información pertinente indicada en el apartado 2.	N/A
5. Las disposiciones de los apartados 1 a 4 no serán aplicables cuando y en la medida en que:	
a) el interesado ya disponga de la información;	N/A
b) la comunicación de dicha información resulte imposible o suponga un esfuerzo desproporcionado, en particular para el tratamiento con fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos, a reserva de las condiciones y garantías indicadas en el artículo 89, apartado 1, o en la medida en que la obligación mencionada en el apartado 1 del presente artículo pueda imposibilitar u obstaculizar gravemente el logro de los objetivos de tal tratamiento. En tales casos, el responsable adoptará medidas adecuadas para proteger los derechos, libertades e intereses legítimos del interesado, inclusive haciendo pública la información;	N/A
c) la obtención o la comunicación esté expresamente establecida por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca medidas adecuadas para proteger los intereses legítimos del interesado, o	N/A
d) cuando los datos personales deban seguir teniendo carácter confidencial sobre la base de una obligación de secreto profesional regulada por el Derecho de la Unión o de los Estados miembros, incluida una obligación de secreto de naturaleza estatutaria.	N/A
Artículo 15 - Derecho de acceso del interesado	
1. El interesado tendrá derecho a obtener del responsable del tratamiento confirmación de si se están tratando o no datos personales que le conciernen y, en tal caso, derecho de acceso a los datos personales y a la siguiente información:	
a) los fines del tratamiento;	100%
b) las categorías de datos personales de que se trate;	100%
c) los destinatarios o las categorías de destinatarios a los que se comunicaron o serán comunicados los datos personales, en particular destinatarios en terceros u organizaciones internacionales;	100%
d) de ser posible, el plazo previsto de conservación de los datos personales o, de no ser posible, los criterios utilizados para determinar este plazo;	100%
e) la existencia del derecho a solicitar del responsable la rectificación o supresión de datos personales o la limitación del tratamiento de datos personales relativos al interesado, o a oponerse a dicho tratamiento;	N/A
f) el derecho a presentar una reclamación ante una autoridad de control;	100%
g) cuando los datos personales no se hayan obtenido del interesado, cualquier información disponible sobre su origen;	N/A
h) la existencia de decisiones automatizadas, incluida la elaboración de perfiles, a que se refiere el artículo 22, apartados 1 y 4, y, al menos en tales casos, información significativa sobre la lógica aplicada, así como la importancia y las consecuencias previstas de dicho tratamiento para el interesado.	N/A

ARTÍCULO RGPD		CMM
2. Cuando se transfieran datos personales a un tercer país o a una organización internacional, el interesado tendrá derecho a ser informado de las garantías adecuadas en virtud del artículo 46 relativas a la transferencia.		N/A
3. El responsable del tratamiento facilitará una copia de los datos personales objeto de tratamiento. El responsable podrá percibir por cualquier otra copia solicitada por el interesado un canon razonable basado en los costes administrativos. Cuando el interesado presente la solicitud por medios electrónicos, y a menos que este solicite que se facilite de otro modo, la información se facilitará en un formato electrónico de uso común.		N/A
4. El derecho a obtener copia mencionado en el apartado 3 no afectará negativamente a los derechos y libertades de otros.		N/A
Artículo 16 - Derecho de rectificación		
El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la rectificación de los datos personales inexactos que le conciernan. Teniendo en cuenta los fines del tratamiento, el interesado tendrá derecho a que se completen los datos personales que sean incompletos, inclusive mediante una declaración adicional.		N/A
Artículo 17 - Derecho de supresión («el derecho al olvido»)		
1. El interesado tendrá derecho a obtener sin dilación indebida del responsable del tratamiento la supresión de los datos personales que le conciernan, el cual estará obligado a suprimir sin dilación indebida los datos personales cuando concorra alguna de las circunstancias siguientes:		
a) los datos personales ya no sean necesarios en relación con los fines para los que fueron recogidos o tratados de otro modo;		80%
b) el interesado retire el consentimiento en que se basa el tratamiento de conformidad con el artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), y este no se base en otro fundamento jurídico;		80%
c) el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 1, y no prevalezcan otros motivos legítimos para el tratamiento, o el interesado se oponga al tratamiento con arreglo al artículo 21, apartado 2;		80%
d) los datos personales hayan sido tratados ilícitamente;		80%
e) los datos personales deban suprimirse para el cumplimiento de una obligación legal establecida en el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento;		90%
f) los datos personales se hayan obtenido en relación con la oferta de servicios de la sociedad de la información mencionados en el artículo 8, apartado 1.		N/A
2. Cuando haya hecho públicos los datos personales y esté obligado, en virtud de lo dispuesto en el apartado 1, a suprimir dichos datos, el responsable del tratamiento, teniendo en cuenta la tecnología disponible y el coste de su aplicación, adoptará medidas razonables, incluidas medidas técnicas, con miras a informar a los responsables que estén tratando los datos personales de la solicitud del interesado de supresión de cualquier enlace a esos datos personales, o cualquier copia o réplica de los mismos.		N/A
Artículo 18 - Derecho a la limitación del tratamiento		
1. El interesado tendrá derecho a obtener del responsable del tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:		
a) el interesado impugne la exactitud de los datos personales, durante un plazo que permita al responsable verificar la exactitud de los mismos;		N/A
b) el tratamiento sea ilícito y el interesado se oponga a la supresión de los datos personales y solicite en su lugar la limitación de su uso;		N/A
c) el responsable ya no necesite los datos personales para los fines del tratamiento, pero el interesado los necesite para la formulación, el ejercicio o la defensa de reclamaciones;		N/A

ARTÍCULO RGPD		CMM
d) el interesado se haya opuesto al tratamiento en virtud del artículo 21, apartado 1, mientras se verifica si los motivos legítimos del responsable prevalecen sobre los del interesado.		N/A
3. Todo interesado que haya obtenido la limitación del tratamiento con arreglo al apartado 1 será informado por el responsable antes del levantamiento de dicha limitación.		N/A
Artículo 19 - Obligación de notificación relativa a la rectificación o supresión de datos personales o la limitación del tratamiento		
El responsable del tratamiento comunicará cualquier rectificación o supresión de datos personales o limitación del tratamiento efectuada con arreglo al artículo 16, al artículo 17, apartado 1, y al artículo 18 a cada uno de los destinatarios a los que se hayan comunicado los datos personales, salvo que sea imposible o exija un esfuerzo desproporcionado. El responsable informará al interesado acerca de dichos destinatarios, si este así lo solicita.		N/A
Artículo 20 - Derecho a la portabilidad de los datos		
1. El interesado tendrá derecho a recibir los datos personales que le incumban, que haya facilitado a un responsable del tratamiento, en un formato estructurado, de uso común y lectura mecánica, y a transmitirlos a otro responsable del tratamiento sin que lo impida el responsable al que se los hubiera facilitado, cuando:		
a) el tratamiento esté basado en el consentimiento con arreglo al artículo 6, apartado 1, letra a), o el artículo 9, apartado 2, letra a), o en un contrato con arreglo al artículo 6, apartado 1, letra b), y		N/A
b) el tratamiento se efectúe por medios automatizados.		N/A
2. Al ejercer su derecho a la portabilidad de los datos de acuerdo con el apartado 1, el interesado tendrá derecho a que los datos personales se transmitan directamente de responsable a responsable cuando sea técnicamente posible.		N/A
Artículo 21 - Derecho de oposición		
1. El interesado tendrá derecho a oponerse en cualquier momento, por motivos relacionados con su situación particular, a que datos personales que le conciernan sean objeto de un tratamiento basado en lo dispuesto en el artículo 6, apartado 1, letras e) o f), incluida la elaboración de perfiles sobre la base de dichas disposiciones. El responsable del tratamiento dejará de tratar los datos personales, salvo que acredite motivos legítimos imperiosos para el tratamiento que prevalezcan sobre los intereses, los derechos y las libertades del interesado, o para la formulación, el ejercicio o la defensa de reclamaciones.		N/A
2. Cuando el tratamiento de datos personales tenga por objeto la mercadotecnia directa, el interesado tendrá derecho a oponerse en todo momento al tratamiento de los datos personales que le conciernan, incluida la elaboración de perfiles en la medida en que esté relacionada con la citada mercadotecnia.		N/A
3. Cuando el interesado se oponga al tratamiento con fines de mercadotecnia directa, los datos personales dejarán de ser tratados para dichos fines.		N/A
4. A más tardar en el momento de la primera comunicación con el interesado, el derecho indicado en los apartados 1 y 2 será mencionado explícitamente al interesado y será presentado claramente y al margen de cualquier otra información.		N/A
5. En el contexto de la utilización de servicios de la sociedad de la información, y no obstante lo dispuesto en la Directiva 2002/58/CE, el interesado podrá ejercer su derecho a oponerse por medios automatizados que apliquen especificaciones técnicas.		N/A
6. Cuando los datos personales se traten con fines de investigación científica o histórica o fines estadísticos de conformidad con el artículo 89, apartado 1, el interesado tendrá derecho, por motivos relacionados con su situación particular, a oponerse al tratamiento de datos personales que le conciernan, salvo que sea necesario para el cumplimiento de una misión realizada por razones de interés público.		N/A
Artículo 22 - Decisiones individuales automatizadas, incluida la elaboración de perfiles		
1. Todo interesado tendrá derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado, incluida la elaboración de perfiles, que produzca efectos jurídicos en él o le afecte significativamente de modo similar.		N/A

ARTÍCULO RGPD	CMM
2. El apartado 1 no se aplicará si la decisión:	
a) es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;	N/A
b) está autorizada por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento y que establezca asimismo medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, o	N/A
c) se basa en el consentimiento explícito del interesado.	N/A
3. En los casos a que se refiere el apartado 2, letras a) y c), el responsable del tratamiento adoptará las medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado, como mínimo el derecho a obtener intervención humana por parte del responsable, a expresar su punto de vista y a impugnar la decisión.	N/A
4. Las decisiones a que se refiere el apartado 2 no se basarán en las categorías especiales de datos personales contempladas en el artículo 9, apartado 1, salvo que se aplique el artículo 9, apartado 2, letra a) o g), y se hayan tomado medidas adecuadas para salvaguardar los derechos y libertades y los intereses legítimos del interesado.	N/A
Artículo 24 - Responsabilidad del responsable del tratamiento	
1. Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el presente Reglamento. Dichas medidas se revisarán y actualizarán cuando sea necesario.	90%
2. Cuando sean proporcionadas en relación con las actividades de tratamiento, entre las medidas mencionadas en el apartado 1 se incluirá la aplicación, por parte del responsable del tratamiento, de las oportunas políticas de protección de datos.	90%
Artículo 25 - Protección de datos desde el diseño y por defecto	
1. Teniendo en cuenta el estado de la técnica, el coste de la aplicación y la naturaleza, ámbito, contexto y fines del tratamiento, así como los riesgos de diversa probabilidad y gravedad que entraña el tratamiento para los derechos y libertades de las personas físicas, el responsable del tratamiento aplicará, tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.	80%
2. El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento. Esta obligación se aplicará a la cantidad de datos personales recogidos, a la extensión de su tratamiento, a su plazo de conservación y a su accesibilidad. Tales medidas garantizarán en particular que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona, a un número indeterminado de personas físicas.	80%
Artículo 26 - Corresponsables del tratamiento	
1. Cuando dos o más responsables determinen conjuntamente los objetivos y los medios del tratamiento serán considerados corresponsables del tratamiento. Los corresponsables determinarán de modo transparente y de mutuo acuerdo sus responsabilidades respectivas en el cumplimiento de las obligaciones impuestas por el presente Reglamento, en particular en cuanto al ejercicio de los derechos del interesado y a sus respectivas obligaciones de suministro de información a que se refieren los artículos 13 y 14, salvo, y en la medida en que, sus responsabilidades respectivas se rijan por el Derecho de la Unión o de los Estados miembros que se les aplique a ellos. Dicho acuerdo podrá designar un punto de contacto para los interesados.	N/A
2. El acuerdo indicado en el apartado 1 reflejará debidamente las funciones y relaciones respectivas de los corresponsables en relación con los interesados. Se pondrán a disposición del interesado los aspectos esenciales del acuerdo.	N/A
Artículo 28 - Encargado del tratamiento	

ARTÍCULO RGPD	CMM
1. Cuando se vaya a realizar un tratamiento por cuenta de un responsable del tratamiento, este elegirá únicamente un encargado que ofrezca garantías suficientes para aplicar medidas técnicas y organizativas apropiadas, de manera que el tratamiento sea conforme con los requisitos del presente Reglamento y garantice la protección de los derechos del interesado.	80%
2. El encargado del tratamiento no recurrirá a otro encargado sin la autorización previa por escrito, específica o general, del responsable. En este último caso, el encargado informará al responsable de cualquier cambio previsto en la incorporación o sustitución de otros encargados, dando así al responsable la oportunidad de oponerse a dichos cambios.	80%
3. El tratamiento por el encargado se regirá por un contrato u otro acto jurídico con arreglo al Derecho de la Unión o de los Estados miembros, que vincule al encargado respecto del responsable y establezca el objeto, la duración, la naturaleza y la finalidad del tratamiento, el tipo de datos personales y categorías de interesados, y las obligaciones y derechos del responsable. Dicho contrato o acto jurídico estipulará, en particular, que el encargado:	
a) tratará los datos personales únicamente siguiendo instrucciones documentadas del responsable, inclusive con respecto a las transferencias de datos personales a un tercer país o una organización internacional, salvo que esté obligado a ello en virtud del Derecho de la Unión o de los Estados miembros que se aplique al encargado; en tal caso, el encargado informará al responsable de esa exigencia legal previa al tratamiento, salvo que tal Derecho lo prohíba por razones importantes de interés público;	80%
b) garantizará que las personas autorizadas para tratar datos personales se hayan comprometido a respetar la confidencialidad o estén sujetas a una obligación de confidencialidad de naturaleza estatutaria;	80%
c) tomará todas las medidas necesarias de conformidad con el artículo 32;	80%
d) respetará las condiciones indicadas en los apartados 2 y 4 para recurrir a otro encargado del tratamiento;	80%
e) asistirá al responsable, teniendo cuenta la naturaleza del tratamiento, a través de medidas técnicas y organizativas apropiadas, siempre que sea posible, para que este pueda cumplir con su obligación de responder a las solicitudes que tengan por objeto el ejercicio de los derechos de los interesados establecidos en el capítulo III;	80%
f) ayudará al responsable a garantizar el cumplimiento de las obligaciones establecidas en los artículos 32 a 36, teniendo en cuenta la naturaleza del tratamiento y la información a disposición del encargado;	80%
g) a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros;	80%
h) pondrá a disposición del responsable toda la información necesaria para demostrar el cumplimiento de las obligaciones establecidas en el presente artículo, así como para permitir y contribuir a la realización de auditorías, incluidas inspecciones, por parte del responsable o de otro auditor autorizado por dicho responsable.	80%
4. Cuando un encargado del tratamiento recurra a otro encargado para llevar a cabo determinadas actividades de tratamiento por cuenta del responsable, se impondrán a este otro encargado, mediante contrato u otro acto jurídico establecido con arreglo al Derecho de la Unión o de los Estados miembros, las mismas obligaciones de protección de datos que las estipuladas en el contrato u otro acto jurídico entre el responsable y el encargado a que se refiere el apartado 3, en particular la prestación de garantías suficientes de aplicación de medidas técnicas y organizativas apropiadas de manera que el tratamiento sea conforme con las disposiciones del presente Reglamento. Si ese otro encargado incumple sus obligaciones de protección de datos, el encargado inicial seguirá siendo plenamente responsable ante el responsable del tratamiento por lo que respecta al cumplimiento de las obligaciones del otro encargado.	80%
9. El contrato u otro acto jurídico a que se refieren los apartados 3 y 4 constará por escrito, inclusive en formato electrónico.	80%
Artículo 29 - Tratamiento bajo la autoridad del responsable o del encargado del tratamiento	

ARTÍCULO RGPD	CMM
El encargado del tratamiento y cualquier persona que actúe bajo la autoridad del responsable o del encargado y tenga acceso a datos personales solo podrán tratar dichos datos siguiendo instrucciones del responsable, a no ser que estén obligados a ello en virtud del Derecho de la Unión o de los Estados miembros.	90%
Artículo 30 - Registro de las actividades de tratamiento	
1. Cada responsable y, en su caso, su representante llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad. Dicho registro deberá contener toda la información indicada a continuación:	
a) el nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos;	80%
b) los fines del tratamiento;	80%
c) una descripción de las categorías de interesados y de las categorías de datos personales;	80%
d) las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales;	80%
e) en su caso, las transferencias de datos personales a un tercer país o una organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;	80%
f) cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos;	80%
g) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 32, apartado 1.	80%
2. Cada encargado y, en su caso, el representante del encargado, llevará un registro de todas las categorías de actividades de tratamiento efectuadas por cuenta de un responsable que contenga:	
a) el nombre y los datos de contacto del encargado o encargados y de cada responsable por cuenta del cual actúe el encargado, y, en su caso, del representante del responsable o del encargado, y del delegado de protección de datos;	80%
b) las categorías de tratamientos efectuados por cuenta de cada responsable;	80%
c) en su caso, las transferencias de datos personales a un tercer país u organización internacional, incluida la identificación de dicho tercer país u organización internacional y, en el caso de las transferencias indicadas en el artículo 49, apartado 1, párrafo segundo, la documentación de garantías adecuadas;	80%
d) cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad a que se refiere el artículo 30, apartado 1.	80%
Artículo 31 - Cooperación con la autoridad de control	
El responsable y el encargado del tratamiento y, en su caso, sus representantes cooperarán con la autoridad de control que lo solicite en el desempeño de sus funciones.	80%
Artículo 32 - Seguridad del tratamiento	
1. Teniendo en cuenta el estado de la técnica, los costes de aplicación, y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas, el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo, que en su caso incluya, entre otros:	80%
Artículo 33 - Notificación de una violación de la seguridad de los datos personales a la autoridad de control	

ARTÍCULO RGPD	CMM
1. En caso de violación de la seguridad de los datos personales, el responsable del tratamiento la notificará a la autoridad de control competente de conformidad con el artículo 55 sin dilación indebida y, de ser posible, a más tardar 72 horas después de que haya tenido constancia de ella, a menos que sea improbable que dicha violación de la seguridad constituya un riesgo para los derechos y las libertades de las personas físicas. Si la notificación a la autoridad de control no tiene lugar en el plazo de 72 horas, deberá ir acompañada de indicación de los motivos de la dilación.	80%
2. El encargado del tratamiento notificará sin dilación indebida al responsable del tratamiento las violaciones de la seguridad de los datos personales de las que tenga conocimiento.	80%
4. Si no fuera posible facilitar la información simultáneamente, y en la medida en que no lo sea, la información se facilitará de manera gradual sin dilación indebida.	80%
5. El responsable del tratamiento documentará cualquier violación de la seguridad de los datos personales, incluidos los hechos relacionados con ella, sus efectos y las medidas correctivas adoptadas. Dicha documentación permitirá a la autoridad de control verificar el cumplimiento de lo dispuesto en el presente artículo.	80%
Artículo 34 - Comunicación de una violación de la seguridad de los datos personales al interesado	
1. Cuando sea probable que la violación de la seguridad de los datos personales entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento la comunicará al interesado sin dilación indebida.	80%
2. La comunicación al interesado contemplada en el apartado 1 del presente artículo describirá en un lenguaje claro y sencillo la naturaleza de la violación de la seguridad de los datos personales y contendrá como mínimo la información y las medidas a que se refiere el artículo 33, apartado 3, letras b), c) y d).	80%
4. Cuando el responsable todavía no haya comunicado al interesado la violación de la seguridad de los datos personales, la autoridad de control, una vez considerada la probabilidad de que tal violación entrañe un alto riesgo, podrá exigirle que lo haga o podrá decidir que se cumple alguna de las condiciones mencionadas en el apartado 3.	80%
Artículo 35 - Evaluación de impacto relativa a la protección de datos	
1. 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, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.	80%
2. El responsable del tratamiento recabará el asesoramiento del delegado de protección de datos, si ha sido nombrado, al realizar la evaluación de impacto relativa a la protección de datos.	80%
3. La evaluación de impacto relativa a la protección de los datos a que se refiere el apartado 1 se requerirá en particular en 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;	N/A
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	80%
c) observación sistemática a gran escala de una zona de acceso público.	N/A
4. La autoridad de control establecerá y publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.	80%

ARTÍCULO RGPD	CMM
5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que no requieren evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.	80%
7. La evaluación deberá incluir como mínimo:	
a) una descripción sistemática de las operaciones de tratamiento previstas y de los fines del tratamiento, inclusive, cuando proceda, el interés legítimo perseguido por el responsable del tratamiento;	90%
b) una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento con respecto a su finalidad;	90%
c) una evaluación de los riesgos para los derechos y libertades de los interesados a que se refiere el apartado 1, y	90%
d) las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de datos personales, y a demostrar la conformidad con el presente Reglamento, teniendo en cuenta los derechos e intereses legítimos de los interesados y de otras personas afectadas.	90%
9. Cuando proceda, el responsable recabará la opinión de los interesados o de sus representantes en relación con el tratamiento previsto, sin perjuicio de la protección de intereses públicos o comerciales o de la seguridad de las operaciones de tratamiento.	50%
11. En caso necesario, el responsable examinará si el tratamiento es conforme con la evaluación de impacto relativa a la protección de datos, al menos cuando exista un cambio del riesgo que representen las operaciones de tratamiento.	50%
Artículo 36 - Consulta previa	
1. El responsable consultará a la autoridad de control antes de proceder al tratamiento cuando una evaluación de impacto relativa a la protección de los datos en virtud del artículo 35 muestre que el tratamiento entrañaría un alto riesgo si el responsable no toma medidas para mitigarlo.	N/A
3. Cuando consulte a la autoridad de control con arreglo al apartado 1, el responsable del tratamiento le facilitará la información siguiente:	
a) en su caso, las responsabilidades respectivas del responsable, los corresponsables y los encargados implicados en el tratamiento, en particular en caso de tratamiento dentro de un grupo empresarial;	N/A
b) los fines y medios del tratamiento previsto;	N/A
c) las medidas y garantías establecidas para proteger los derechos y libertades de los interesados de conformidad con el presente Reglamento;	N/A
d) en su caso, los datos de contacto del delegado de protección de datos;	N/A
e) la evaluación de impacto relativa a la protección de datos establecida en el artículo 35, y	N/A
f) cualquier otra información que solicite la autoridad de control.	N/A
Artículo 37 - Designación del delegado de protección de datos	
1. El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:	
a) el tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial;	100%
b) las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o	100%
c) las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales con arreglo al artículo 9 y de datos relativos a condenas e infracciones penales a que se refiere el artículo 10.	100%
5. El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar las funciones indicadas en el artículo 39.	100%

ARTÍCULO RGPD	CMM
7. El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.	100%
Artículo 38 - Posición del delegado de protección de datos	
1. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos participe de forma adecuada y en tiempo oportuno en todas las cuestiones relativas a la protección de datos personales.	80%
2. El responsable y el encargado del tratamiento respaldarán al delegado de protección de datos en el desempeño de las funciones mencionadas en el artículo 39, facilitando los recursos necesarios para el desempeño de dichas funciones y el acceso a los datos personales y a las operaciones de tratamiento, y para el mantenimiento de sus conocimientos especializados.	80%
3. El responsable y el encargado del tratamiento garantizarán que el delegado de protección de datos no reciba ninguna instrucción en lo que respecta al desempeño de dichas funciones. No será destituido ni sancionado por el responsable o el encargado por desempeñar sus funciones. El delegado de protección de datos rendirá cuentas directamente al más alto nivel jerárquico del responsable o encargado.	80%
4. Los interesados podrán ponerse en contacto con el delegado de protección de datos por lo que respecta a todas las cuestiones relativas al tratamiento de sus datos personales y al ejercicio de sus derechos al amparo del presente Reglamento.	80%
5. El delegado de protección de datos estará obligado a mantener el secreto o la confidencialidad en lo que respecta al desempeño de sus funciones, de conformidad con el Derecho de la Unión o de los Estados miembros.	80%
6. El delegado de protección de datos podrá desempeñar otras funciones y cometidos. El responsable o encargado del tratamiento garantizará que dichas funciones y cometidos no den lugar a conflicto de intereses.	80%
Artículo 39 - Funciones del delegado de protección de datos	
1. El delegado de protección de datos tendrá como mínimo las siguientes funciones:	
a) informar y asesorar al responsable o al encargado del tratamiento y a los empleados que se ocupen del tratamiento de las obligaciones que les incumben en virtud del presente Reglamento y de otras disposiciones de protección de datos de la Unión o de los Estados miembros;	80%
b) supervisar el cumplimiento de lo dispuesto en el presente Reglamento, de otras disposiciones de protección de datos de la Unión o de los Estados miembros y de las políticas del responsable o del encargado del tratamiento en materia de protección de datos personales, incluida la asignación de responsabilidades, la concienciación y formación del personal que participa en las operaciones de tratamiento, y las auditorías correspondientes;	80%
c) ofrecer el asesoramiento que se le solicite acerca de la evaluación de impacto relativa a la protección de datos y supervisar su aplicación de conformidad con el artículo 35;	80%
d) cooperar con la autoridad de control;	80%
2. El delegado de protección de datos desempeñará sus funciones prestando la debida atención a los riesgos asociados a las operaciones de tratamiento, teniendo en cuenta la naturaleza, el alcance, el contexto y fines del tratamiento.	80%
Artículo 45 - Transferencias basadas en una decisión de adecuación	
1. Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garanticen un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.	N/A

ARTÍCULO RGPD	CMM
5. Cuando la información disponible, en particular tras la revisión a que se refiere el apartado 3 del presente artículo, muestre que un tercer país, un territorio o un sector específico de ese tercer país, o una organización internacional ya no garantiza un nivel de protección adecuado a tenor del apartado 2 del presente artículo, la Comisión, mediante actos de ejecución, derogará, modificará o suspenderá, en la medida necesaria y sin efecto retroactivo, la decisión a que se refiere el apartado 3 del presente artículo. Dichos actos de ejecución se adoptarán de acuerdo con el procedimiento de examen a que se refiere el artículo 93, apartado 2.	N/A
Artículo 46 - Transferencias mediante garantías adecuadas	
1. A falta de decisión con arreglo al artículo 45, apartado 3, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas.	N/A
2. Las garantías adecuadas con arreglo al apartado 1 podrán ser aportadas, sin que se requiera ninguna autorización expresa de una autoridad de control, por:	
a) un instrumento jurídicamente vinculante y exigible entre las autoridades u organismos públicos;	N/A
b) normas corporativas vinculantes de conformidad con el artículo 47;	
c) cláusulas tipo de protección de datos adoptadas por la Comisión de conformidad con el procedimiento de examen a que se refiere el artículo 93, apartado 2;	N/A
d) cláusulas tipo de protección de datos adoptadas por una autoridad de control y aprobadas por la Comisión con arreglo al procedimiento de examen a que se refiere en el artículo 93, apartado 2;	N/A
e) un código de conducta aprobado con arreglo al artículo 40, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados, o	N/A
f) un mecanismo de certificación aprobado con arreglo al artículo 42, junto con compromisos vinculantes y exigibles del responsable o el encargado del tratamiento en el tercer país de aplicar garantías adecuadas, incluidas la relativas a los derechos de los interesados.	N/A
3. Siempre que exista autorización de la autoridad de control competente, las garantías adecuadas contempladas en el apartado 1 podrán igualmente ser aportadas, en particular, mediante:	
a) cláusulas contractuales entre el responsable o el encargado y el responsable, encargado o destinatario de los datos personales en el tercer país u organización internacional, o	N/A
b) disposiciones que se incorporen en acuerdos administrativos entre las autoridades u organismos públicos que incluyan derechos efectivos y exigibles para los interesados.	N/A
Artículo 47 - Normas corporativas vinculantes	
1. La autoridad de control competente aprobará normas corporativas vinculantes de conformidad con el mecanismo de coherencia establecido en el artículo 63, siempre que estas:	
a) sean jurídicamente vinculantes y se apliquen y sean cumplidas por todos los miembros correspondientes del grupo empresarial o de la unión de empresas dedicadas a una actividad económica conjunta, incluidos sus empleados;	N/A
b) confieran expresamente a los interesados derechos exigibles en relación con el tratamiento de sus datos personales, y c) cumplan los requisitos establecidos en el apartado 2.	N/A
3. La Comisión podrá especificar el formato y los procedimientos para el intercambio de información entre los responsables, los encargados y las autoridades de control en relación con las normas corporativas vinculantes a tenor de lo dispuesto en el presente artículo. Dichos actos de ejecución se adoptarán con arreglo al procedimiento de examen a que se refiere el artículo 93, apartado 2.	N/A
Artículo 48 - Transferencias o comunicaciones no autorizadas por el Derecho de la Unión	

ARTÍCULO RGPD	CMM
Cualquier sentencia de un órgano jurisdiccional o decisión de una autoridad administrativa de un tercer país que exijan que un responsable o encargado del tratamiento transfiera o comunique datos personales únicamente será reconocida o ejecutable en cualquier modo si se basa en un acuerdo internacional, como un tratado de asistencia jurídica mutua, vigente entre el país tercero requirente y la Unión o un Estado miembro, sin perjuicio de otros motivos para la transferencia al amparo del presente capítulo.	N/A
Artículo 49 - Excepciones para situaciones específicas	
1. En ausencia de una decisión de adecuación de conformidad con el artículo 45, apartado 3, o de garantías adecuadas de conformidad con el artículo 46, incluidas las normas corporativas vinculantes, una transferencia o un conjunto de transferencias de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones siguientes:	
a) el interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas;	N/A
b) la transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud del interesado;	N/A
c) la transferencia sea necesaria para la celebración o ejecución de un contrato, en interés del interesado, entre el responsable del tratamiento y otra persona física o jurídica;	N/A
d) la transferencia sea necesaria por razones importantes de interés público;	N/A
e) la transferencia sea necesaria para la formulación, el ejercicio o la defensa de reclamaciones;	N/A
f) la transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas, cuando el interesado esté física o jurídicamente incapacitado para dar su consentimiento;	N/A
g) la transferencia se realice desde un registro público que, con arreglo al Derecho de la Unión o de los Estados miembros, tenga por objeto facilitar información al público y esté abierto a la consulta del público en general o de cualquier persona que pueda acreditar un interés legítimo, pero sólo en la medida en que se cumplan, en cada caso particular, las condiciones que establece el Derecho de la Unión o de los Estados miembros para la consulta.	N/A
2. Una transferencia efectuada de conformidad con el apartado 1, párrafo primero, letra g), no abarcará la totalidad de los datos personales ni categorías enteras de datos personales contenidos en el registro. Si la finalidad del registro es la consulta por parte de personas que tengan un interés legítimo, la transferencia solo se efectuará a solicitud de dichas personas o si estas han de ser las destinatarias.	N/A
3. En el apartado 1, el párrafo primero, letras a), b) y c), y el párrafo segundo no serán aplicables a las actividades llevadas a cabo por las autoridades públicas en el ejercicio de sus poderes públicos.	N/A
4. El interés público contemplado en el apartado 1, párrafo primero, letra d), será reconocido por el Derecho de la Unión o de los Estados miembros que se aplique al responsable del tratamiento.	N/A
6. El responsable o el encargado del tratamiento documentarán en los registros indicados en el artículo 30 la evaluación y las garantías apropiadas a que se refiere el apartado 1, párrafo segundo, del presente artículo.	N/A

Tabla 16 Madurez artículos RGPD

Anexo IV – Información Modificada de Amenazas

En este anexo se recogen las modificaciones efectuadas sobre la frecuencia de ocurrencia de determinadas amenazas respecto a los valores estándar registrados en la Herramienta PILAR, para realizar el presente Análisis de Riesgos.

Los cambios realizados están motivados por la consideración de que alguno de los valores por defecto que proporciona PILAR son superiores a los que deberían establecerse para el Servicio Radar Covid19.

El significado de los distintos valores que puede tomar la frecuencia de las amenazas es el siguiente:

Frecuencia	Descripción
100	Casi seguro
10	Muy alta
1	Posible
0,1	Poco probable.
0,01	Muy rara

Tabla 17 Descripción valores frecuencia

Para determinar los nuevos valores de frecuencia se han tenido en cuenta fundamentalmente los siguientes bloques de información contemplados, entre otros, en la Herramienta PILAR:

- Equipamiento Hardware
- Instalaciones
- Personal
- Terceros

En relación con los dos primeros, las modificaciones han consistido básicamente en disminuir la frecuencia de 'Posible' a 'Poco probable', motivado porque ambos están estrechamente relacionados con la plataforma en la nube de Amazon: Amazon Web Services (AWS).

AWS es una plataforma tecnológica segura con certificaciones y auditorías reconocidas en el sector, como por ejemplo: PCI DSS Nivel 1, ISO 27001, FISMA Moderate, etc. Las certificaciones y acreditaciones, el cifrado de datos en reposo y en tránsito, los módulos de seguridad hardware y una fuerte seguridad física contribuyen a crear un modo seguro de administrar la infraestructura TI.

AWS está implantado en 24 regiones geográficas y cada región tiene diferentes "zonas de disponibilidad" (centros de datos que proporcionan los servicios AWS).

Dispone de una red diseñada para proteger la información, identidades, aplicaciones y dispositivos. Identifica amenazas mediante la monitorización continua de la actividad de la red. Dispone de protección frente ataques DDoS. Filtra el tráfico malintencionado.

Las amenazas implicadas en la modificación efectuada se enumeran a continuación

- Abuso de privilegios de acceso
- Ataque destructivo
- Avería de origen físico o lógico
- Caída del sistema por agotamiento de recursos
- Condiciones inadecuadas de temperatura o humedad

- Contaminación electromagnética
- Contaminación medioambiental
- Corte del suministro eléctrico
- Daños por agua
- Denegación de servicio
- Desastres industriales
- Desastres naturales
- Emanaciones electromagnéticas
- Fallo de servicios de comunicaciones
- Fuego
- Interrupción de otros servicios o suministros esenciales
- Ocupación enemiga
- Pérdida de equipos
- Robo de equipos
- Suplantación de la Identidad

Por otra parte en relación con los grupos: Personal y Terceros, las modificaciones también han consistido básicamente en disminuir la frecuencia de 'Posible' a 'Poco probable', motivado por el tipo de información tratado por la aplicación y el perfil del personal implicado en su tratamiento (Usuarios, administradores, desarrolladores, etc.).

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

Las amenazas implicadas en la modificación efectuada se enumeran a continuación, entre las que destacan fundamentalmente las relacionadas con la información:

- Alteración de la información
- Destrucción de la información
- Errores de mantenimiento
- Extorsión
- Fugas de información
- Indisponibilidad del personal
- Ingeniería social
- Modificación de la información
- Revelación de información

La siguiente tabla muestra las frecuencias que han sido modificadas. Por cada una de ellas se indica el valor estándar registrado por la Herramienta PILAR y el nuevo valor incluido para realizar el presente análisis de riesgos:

VALORES POR DEFECTO PILAR				VALOR MODIFICADO
family	threat	Descripción de amenazas	likely	likely
L	A.6	Abuso de privilegios de acceso	1	0,1
S.3rd	E.15	Alteración de la información	1	0,1
P	E.15	Alteración de la información	1	0,1
HW	A.26	Ataque destructivo	1	0,1
HW	I.5	Avería de origen físico o lógico	1	0,1
HW	E.24	Caída del sistema por agotamiento de recursos	10	1
HW	I.7	Condiciones inadecuadas de temperatura o humedad	1	0,1

VALORES POR DEFECTO PILAR				VALOR MODIFICADO
family	threat	Descripción de amenazas	likely	likely
HW	I.4	Contaminación electromagnética	1	0,1
L	I.3	Contaminación medioambiental	1	0,1
HW	I.6	Corte del suministro eléctrico	1	0,1
HW	I.2	Daños por agua	0,5	0,1
L	N.2	Daños por agua	1	0,1
L	I.2	Daños por agua	1	0,1
S.prov	A.24	Denegación de servicio	10	2
HW	A.24	Denegación de servicio	2	1
COM	A.24	Denegación de servicio	10	2
HW	I.*	Desastres industriales	0,5	0,01
L	I.*	Desastres industriales	1	0,01
HW	N.*	Desastres naturales	0,1	0,01
L	N.*	Desastres naturales	0,5	0,01
S.3rd	E.18	Destrucción de la información	1	0,1
S.3rd	A.18	Destrucción de la información	1	0,1
P	E.18	Destrucción de la información	1	0,1
P	A.18	Destrucción de la información	1	0,1
HW	I.11	Emanaciones electromagnéticas	1	0,1
SW	E.21	Errores de mantenimiento	10	1
P	A.29	Extorsión	0,9	0,1
P.ue	A.29	Extorsión	0,9	0,1
P.ui	A.29	Extorsión	0,9	0,1
P.op	A.29	Extorsión	0,9	0,1
P.adm	A.29	Extorsión	0,9	0,1
P.com	A.29	Extorsión	0,9	0,1
P.dba	A.29	Extorsión	0,9	0,1
P.sec	A.29	Extorsión	0,9	0,1
P.dev	A.29	Extorsión	0,9	0,1
S.3rd.ISP	I.8	Fallo de servicios de comunicaciones	1	0,1
S.3rd.comms	I.8	Fallo de servicios de comunicaciones	1	0,1
HW	I.1	Fuego	0,5	0,1
L	N.1	Fuego	1	0,1
L	I.1	Fuego	1	0,1
S.3rd	E.19	Fugas de información	1	0,1
P	E.19	Fugas de información	1	0,1
P.ue	E.19	Fugas de información	1	0,1
P.ui	E.19	Fugas de información	1	0,1
P.op	E.19	Fugas de información	1	0,1
P.adm	E.19	Fugas de información	1	0,1
P.com	E.19	Fugas de información	1	0,1
P.dba	E.19	Fugas de información	1	0,1
P.sec	E.19	Fugas de información	1	0,1
P.dev	E.19	Fugas de información	1	0,1

VALORES POR DEFECTO PILAR				VALOR MODIFICADO
family	threat	Descripción de amenazas	likely	likely
P.ue	A.28	Indisponibilidad del personal	0,1	0,5
P.ui	E.28	Indisponibilidad del personal	1	0,5
P.op	E.28	Indisponibilidad del personal	1	0,5
P.adm	E.28	Indisponibilidad del personal	1	0,5
P.com	E.28	Indisponibilidad del personal	1	0,5
P.dba	E.28	Indisponibilidad del personal	1	0,5
P.sec	E.28	Indisponibilidad del personal	1	0,5
P.dev	E.28	Indisponibilidad del personal	1	0,5
P	A.30	Ingeniería social	0,5	0,1
P.ue	A.30	Ingeniería social	1	0,1
P.ui	A.30	Ingeniería social	0,5	0,1
P.op	A.30	Ingeniería social	0,5	0,1
P.adm	A.30	Ingeniería social	0,5	0,1
P.dba	A.30	Ingeniería social	0,5	0,1
P.sec	A.30	Ingeniería social	0,5	0,1
P.dev	A.30	Ingeniería social	0,5	0,1
S.3rd	I.9	Interrupción de otros servicios o suministros esenciales	1	0,1
S.3rd	A.15	Modificación de la información	1	0,1
P	A.15	Modificación de la información	1	0,1
L	A.27	Ocupación enemiga	1	0
HW	E.25	Pérdida de equipos	1	0,1
S.3rd	A.13	Repudio	1	0,1
S.3rd	A.19	Revelación de información	1	0,1
P	A.19	Revelación de información	1	0,1
P.ue	A.19	Revelación de información	5	0,1
P.ui	A.19	Revelación de información	10	0,1
P.op	A.19	Revelación de información	10	0,1
P.adm	A.19	Revelación de información	10	0,1
P.com	A.19	Revelación de información	1	0,1
P.dba	A.19	Revelación de información	10	0,1
P.sec	A.19	Revelación de información	10	0,1
P.dev	A.19	Revelación de información	10	0,1
S.3rd	A.24	Robo	1	0,1
HW	A.25	Robo de equipos	0,5	0,01
S.prov	A.5	Suplantación de la Identidad	1	0,1
S.3rd	A.5	Suplantación de la Identidad	0,2	0,1
COM	A.5	Suplantación de la Identidad	1	0,1
L	A.7	Uso no previsto	1	0,1

Tabla 18 Relación de Amenazas con la frecuencia por defecto y la frecuencia modificada

En cuanto a las amenazas correspondientes a los Datos de Carácter Personal se han utilizado las amenazas estándar registradas en la Herramienta PILAR, 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 superiores 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

Tabla 19 Amenazas de Datos de Carácter Personal

