Análisis de Riesgos

Sistema de Información Radar Covid19

Agosto de 2020

ÍNDICE

RELACIÓN DE TABLAS

RELACIÓN DE ILUSTRACIONES

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.

> *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.*

Para la realización del presente Análisis de Riesgos se ha utilizado la información relativa al diseño y desarrollo del **Sistema de Información Radar Covid19** y toda aquella información aportada por el **Ministerio de Asuntos Económicos y Transformación Digital**, a través de los responsables correspondientes de la **Secretaría de Estado de Digitalización e Inteligencia Artificial**.

1.1 Objetivos

El presente documento, encuadrado en el **Plan de Adecuación al Esquema Nacional de Seguridad del Sistema de Información Radar Covid19**, tiene como objetivo exponer los resultados del Análisis de Riesgos realizado a dicho Sistema de Información dentro del alcance del ENS.

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

1.2 Audiencia

El presente documento va dirigido a:

- Comité de Seguridad de la Información, formado por:
  - Responsable de Seguridad
  - Responsable de Sistemas
  - Responsable de la Información
  - Responsable del Servicio.
- Aquellas personas que la Secretaria del Estado de Digitalización e Inteligencia Artificial estime conveniente.

1.3 Alcance

El alcance del presenta Análisis de Riesgos comprende el **Sistema de Información Radar Covid19**. Constituido por un aplicación contact tracing Bluetooth para la Secretaría de Estado de Digitalización e Inteligencia Artificial (SEDIA).

1.4 Estructura del documento

El documento se estructura en tres apartados generales:

- Introducción: Es el presente apartado, donde se establecen los objetivos del documento, el alcance, la estructura y la audiencia a la que va dirigido.
- 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.
- Análisis de Riesgos: Descripción del trabajo realizado:
    - Categorización de Activos
    - Categorización de Amenazas
    - Categorización de Salvaguardas
    - Estimación del Estado del Riesgo
- Conclusiones: Resultados del Análisis de Riesgos y recomendaciones para eliminarlos y/o mitigarlos.
- Anexos: Información complementaria al presente documento.

1.5 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:

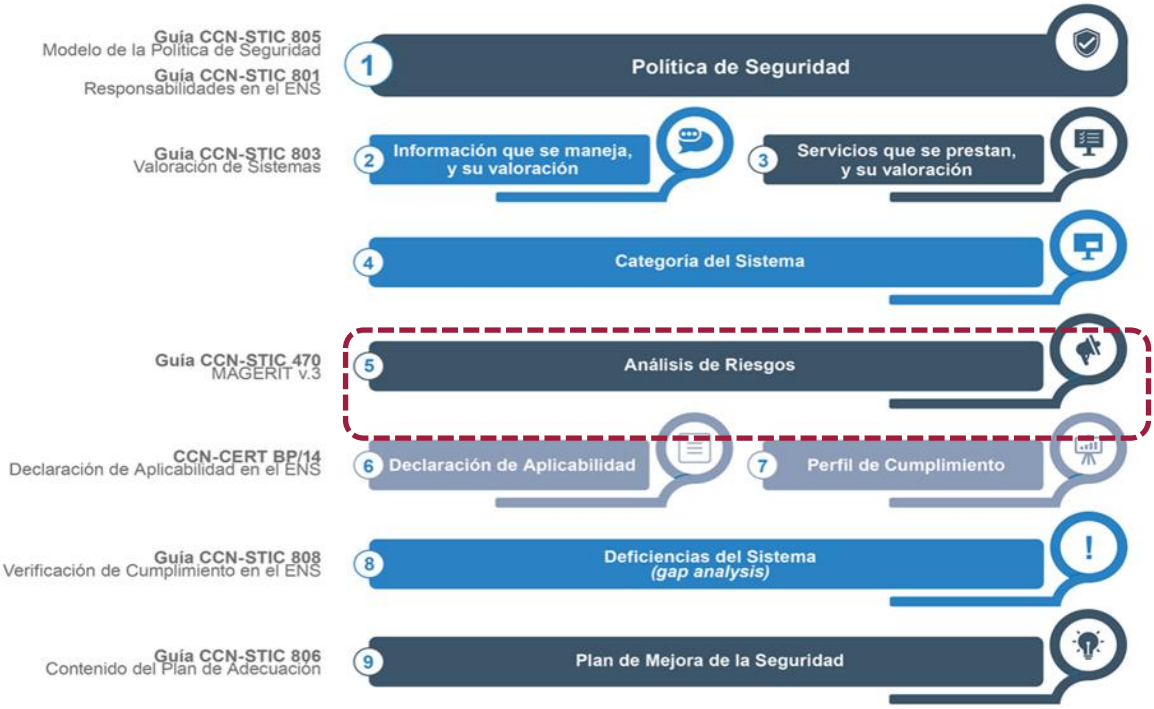

Ilustración 1 Plan de Adecuación al ENS

Para la realización del Análisis de Riesgos se han mantenido diferentes reuniones con los responsables de negocio, responsables de la información y responsables técnicos involucrados en el Desarrollo de la **Aplicación Radar Covid19**. Como resultado de esta actividad se han cumplimentado los Cuestionarios de Negocio y los Cuestionarios Técnicos en los que 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.

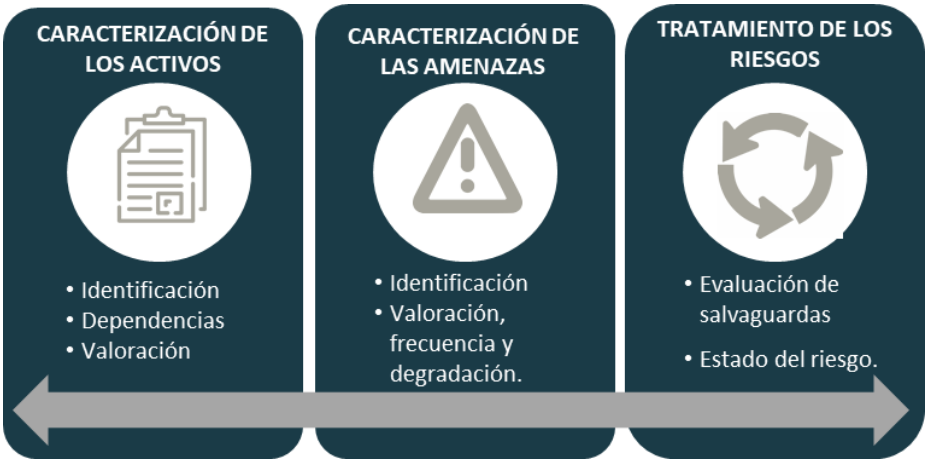

Ilustración 2 Fases del Análisis de Riesgos

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 con Activo Esencial el Sistema de Información *[0001] Sistema de Información Radar Covid19*.

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

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

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

La valoración se ha determinado teniendo en cuenta la Guía CCN-STIC 803 ENS "*Valoración de los sistemas*" y también se recoge en el *Anexo I: Inventario de Activos*, 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*.

Por último, se han establecido las **dependencias entre activos** (Véase *Anexo I: Inventario de Activos*). Se dice que un "activo superior" depende de otro "activo inferior" cuando las necesidades de seguridad del superior se reflejan en las necesidades de seguridad del inferior.

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

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 Sistemas 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, nos 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
80 %	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
10	Frecuente
1	Normal
0,1	Poco frecuente

Tabla 2 Frecuencia de Amenazas

Con la información obtenida hasta el momento se puede determinar el **Riesgo Potencial**, como la medida del daño probable sobre un sistema.

2.3 Tratamiento de los Riesgos – 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 conjuran simplemente con una organización adecuada, otras requieren elementos técnicos (programas o equipos), otras requieren seguridad física, política de personal, etc.

La **caracterización** de las salvaguardas se ha realizado mediante la cumplimentación de un Cuestionario Técnico basado en el Anexo II: *Medidas de Seguridad*, del Esquema Nacional de Seguridad (RD 951/2015), que constituyen las medidas implementadas por la Herramienta

PILAR. Así mismo, para la definición de los controles se ha tenido en cuenta Guía CCN-STIC-808: *Verificación del Cumplimiento del ENS*.

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

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

Tabla 4 Niveles de Madurez

2.4 Tratamiento de los Riesgos – 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.

El detalle de los **riesgos potenciales** asociados a los activos de información se recogen en el archivo: Riesgos Potenciales.

El valor del Riesgo Potencial obtenido de la Herramienta PILAR: **{6,3}**

2.4.2 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.

El detalle de los **riesgos residuales** asociados a los activos de información se recogen en el archivo: Riesgos Residuales.

El valor del Riesgo Residual obtenido de la Herramienta PILAR: **{5,0}**

2.4.3 Riesgo Objetivo ENS

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. Para establecer los objetivos se debe tener en cuenta el nivel de madurez mínimo exigido por el Esquema Nacional de Seguridad (Véase la Guía CCN-STIC 824: *Informe Nacional del Estado de Seguridad de los Sistemas TIC*):

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

El detalle de los **riesgos objetivos propuestos** asociados a los activos de información se recogen en el archivo: Riesgos Objetivo.

El valor del Riesgo Objetivo obtenido de la Herramienta PILAR: **{2,5}**

Anexo I – Inventario de Activos

Inventario de Activos

INVENTARIO DE ACTIVOS		
TIPO	CÓDIGO	NOMBREDE ACTIVO
[B] Activos esenciales		
	[001]	Sistema de Información Radar Covid20
[SE] Servicios Externos		
	[SE-0001]	Servicio Central de Gestión de Balizas
	[SE-0002]	Servicio Central de Validación de Positivos
	[SE-0003]	Repositorio de descargas (ANDROID STORE)
	[SE-0004]	Repositorio de descargas (APPLE STORE)
[E] Equipamiento		
[SW] Aplicaciones		
	[SW-0001]	App Radar Covil20
[HW] Equipos		
	[HW-0001]	Teléfono Móvil
	[HW-0002]	Equipos Físicos del Ministerio
	[HW-0003]	Equipos Físicos de Terceros
[COM] Comunicaciones		
	[COM-0001]	Redes de Comunicaciones
[SS] Servicios subcontratados		
	[SS-0001]	Desarollo y Mantenimiento de la App
[L] Instalaciones		
	[L-0001]	Instalaciones del Ministerio
	[L-0002]	Instalaciones de Terceros
[P] Personal		
	[P-0001]	Ciudadanos
	[P-0002]	Administradores / Operadores
	[P-0003]	Desarrolladores

Clases de Activos

CLASES DE ACTIVOS			
TIPO	**CÓDIGO**	**NOMBREDE ACTIVO**	**CLASE**
[B] Activos esenciales			
	[001]	Sistema de Información Radar Covid20	{essential{info.adm,service},D}
[SE] Servicios Externos			
	[SE-0001]	Servicio Central de Gestión de Balizas	{Servicios}
	[SE-0002]	Servicio Central de Validación de Positivos	{Servicios}
	[SE-0003]	Repositorio de descargas (ANDROID STORE)	{Servicios}
	[SE-0004]	Repositorio de descargas (APPLE STORE)	{Servicios}
[E] Equipamiento			
[SW] Aplicaciones			
	[SW-0001]	App Radar Covil20	{Aplicaciones (Software}
[HW] Equipos			
	[HW-0001]	Teléfono Móvil	{Equipamiento Informático (Hardware)}
	[HW-0002]	Equipos Físicos del Ministerio	{Equipamiento Informático (Hardware)}
	[HW-0003]	Equipos Físicos de Terceros	{Equipamiento Informático (Hardware)}
[COM] Comunicaciones			
	[COM-0001]	Redes de Comunicaciones	{Red Telefónica, WIFI, Telefonía Móvil}
[SS] Servicios subcontratados			
	[SS-0001]	Desarollo y Mantenimiento de la App	{Servicios{Contratos a Terceros}}
[L] Instalaciones			
	[L-0001]	Instalaciones del Ministerio	{Recinto, Edificio}
	[L-0002]	Instalaciones de Terceros	{Recinto, Edificio}
[P] Personal			
	[P-0001]	Ciudadanos	{Personal{ue}}
	[P-0002]	Administradores / Operadores	{Personal{op, adm, com, dba, sec}}
	[P-0003]	Desarrolladores	{Personal{dev, prov}}

Dependencias entre Activos

DEPENDENCIAS ENTRE ACTIVOS	
ACTIVOS	**DEPENDENCIAS**
[001] Sistema de Información Radar Covid20	
	[SE-0001] Servicio Central de Gestión de Balizas
	[SW-0001] App Radar Covil19
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[HW-0002] Equipos Físicos del Ministerio
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
	[SE-0002] Servicio Central de Validación de Positivos
	[SW-0001] App Radar Covil19
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[HW-0002] Equipos Físicos del Ministerio
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
	[SE-0003] Repositorio de descargas (ANDROID STORE)
	[HW-0003] Equipos Físicos de Terceros
	[L-0002] Instalaciones de Terceros
	[SE-0004] Repositorio de descargas (APPLE STORE)
	[HW-0003] Equipos Físicos de Terceros
	[L-0002] Instalaciones de Terceros
	[COM-0001] Redes de Comunicaciones
	[SS-0001] Desarollo y Mantenimiento de la App
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[SE-0001] Servicio Central de Gestión de Balizas	
	[SW-0001] App Radar Covil19
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[HW-0002] Equipos Físicos del Ministerio
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores

DEPENDENCIAS ENTRE ACTIVOS	
ACTIVOS	**DEPENDENCIAS**
[SE-0002] Servicio Central de Validación de Positivos	
	[SW-0001] App Radar Covil19
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[HW-0002] Equipos Físicos del Ministerio
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[SE-0003] Repositorio de descargas (ANDROID STORE)	
	[HW-0003] Equipos Físicos de Terceros
	[L-0002] Instalaciones de Terceros
[SE-0004] Repositorio de descargas (APPLE STORE)	
	[HW-0003] Equipos Físicos de Terceros
	[L-0002] Instalaciones de Terceros
[SW-0001] App Radar Covil20	
	[HW-0001] Teléfono Móvil
	[P-0001] Ciudadanos
	[HW-0002] Equipos Físicos del Ministerio
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[HW-0001] Teléfono Móvil	
	[P-0001] Ciudadanos
[HW-0002] Equipos Físicos del Ministerio	
	[L-0001] Instalaciones del Ministerio
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[HW-0003] Equipos Físicos de Terceros	
	[L-0002] Instalaciones de Terceros
[COM-0001] Redes de Comunicaciones	
[SS-0001] Desarollo y Mantenimiento de la App	
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[L-0001] Instalaciones del Ministerio	
	[P-0001] Ciudadanos
	[P-0002] Administradores / Operadores
	[P-0003] Desarrolladores
[L-0002] Instalaciones de Terceros	
[P-0001] Ciudadanos	
[P-0002] Administradores / Operadores	
[P-0003] Desarrolladores	

Valoración de Sistemas de Información

VALORACIÓN DE SISTEMAS DE INFORMACIÓN						
SISTEMAS DE INFORMACIÓN	A	C	I	D	A	VALORACIÓN
[0001] Sistema de Información Radar Covid19	ALTO	ALTO	ALTO	MEDIO	MEDIO	ALTO
	ALTO	ALTO	ALTO	MEDIO	MEDIO	

Anexo II – Criterios de Valoración de Sistemas de Información

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 necesiten 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.

Anexo III – Caracterización de Salvaguardas

ESQUEMA NACIONAL DE SEGURIDAD			
REF.	MEDIDAS		**CMM**
org	MARCO ORGANIZATIVO		
	org.1	Política de seguridad	L3
	org.2	Normativa de seguridad	L3
	org.3	Procedimientos de seguridad	L3
	org.4	Proceso de autorización	L3
op	MARCO OPERACIONAL		
op.pl	Planificación		
	op.pl.1	Análisis de riesgos	L3
	op.pl.2	Arquitectura de seguridad	L4
	op.pl.3	Adquisición de nuevos componentes	n.a. ()
	op.pl.4	Dimensionamiento / gestión de capacidades	L2
	op.pl.5	Componentes certificados	n.a. ()
op.acc	Control de acceso		
	op.acc.1	Identificación	n.a. (_-L0)
	op.acc.2	Requisitos de acceso	L0
	op.acc.3	Segregación de funciones y tareas	L0
	op.acc.4	Proceso de gestión de derechos de acceso	(_-L0)
	op.acc.5	Mecanismo de autenticación	L0
	op.acc.6	Acceso local (Local Logon)	L3 (L3-L4)
	op.acc.7	Acceso remoto (Remote Login)	L3-L4 (L3-L5)
op.exp	Explotación		
	op.exp.1	Inventario de activos	L3-L4 (L3-L5)
	op.exp.2	Configuración de seguridad	L4 (L3-L4)
	op.exp.3	Gestión de la configuración	L3 (L3-L5)
	op.exp.4	Mantenimiento	L3 (L3-L4)
	op.exp.5	Gestión de cambios	L4
	op.exp.6	Protección frente a código dañino	L4 (L3-L4)
	op.exp.7	Gestión de incidentes	L3 (L3-L4)
	op.exp.8	Registro de la actividad de los usuarios	L4
	op.exp.9	Registro de la gestión de incidentes	L4
	op.exp.10	Protección de los registros de actividad	L3
	op.exp.11	Protección de claves criptográficas	n.a. (_-L5)

ESQUEMA NACIONAL DE SEGURIDAD			
REF.	MEDIDAS		**CMM**
op.ext	Servicios externos		
	op.ext.1	Contratación y acuerdos de nivel de servicio	n.a. ()
	op.ext.2	Gestión diaria	n.a. ()
	op.ext.9	Medios alternativos	L3
op.cont	Continuidad del servicio		
	op.cont.1	Análisis de impacto	n.a. ()
	op.cont.2	Plan de continuidad	n.a. ()
	op.cont.3	Pruebas periódicas	n.a. ()
op.mon	Monitorización del sistema		
	op.mon.1	Detección de intrusión	n.a. ()
	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	n.a. (_-L3)
	mp.if.2	Identificación de las personas	n.a. ()
	mp.if.3	Acondicionamiento de los locales	n.a. ()
	mp.if.4	Energía eléctrica	n.a. ()
	mp.if.5	Protección frente a incendios	n.a. ()
	mp.if.6	Protección frente a inundaciones	n.a. ()
	mp.if.7	Registro de entrada y salida de equipamiento	n.a. ()
	mp.if.9	Instalaciones alternativas	L3
mp.per	Gestión del personal		
	mp.per.1	Caracterización del puesto de trabajo	L3
	mp.per.2	Deberes y obligaciones	L3
	mp.per.3	Concienciación	L3
	mp.per.4	Formación	L3
	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	n.a. ()
	mp.eq.3	Protección de portátiles	n.a. (_-L4)
	mp.eq.9	Medios alternativos	n.a. ()
mp.com	Protección de las comunicaciones		
	mp.com.1	Perímetro seguro	L4 (L3-L4)
	mp.com.2	Protección de la confidencialidad	L4 (L5)

ESQUEMA NACIONAL DE SEGURIDAD			
REF.	MEDIDAS		**CMM**
	mp.com.3	Protección de la autenticidad y de la integridad	L3
	mp.com.4	Segregación de redes	L3 (L3-L4)
	mp.com.9	Medios alternativos	L3
mp.si	Protección de los soportes de información		
	mp.si.1	Etiquetado	n.a. ()
	mp.si.2	Criptografía	n.a. (_-L3)
	mp.si.3	Custodia	n.a. (_-L3)
	mp.si.4	Transporte	L3
	mp.si.5	Borrado y destrucción	L2
mp.sw	Protección de las aplicaciones informáticas		
	mp.sw.1	Desarrollo de aplicaciones	L3 (L3-L5)
	mp.sw.2	Aceptación y puesta en servicio	L5
mp.info	Protección de la información		
	mp.info.1	Datos de carácter personal	n.a.
	mp.info.2	Calificación de la información	L0
	mp.info.3	Cifrado de la información	L4-L5 (_-L5)
	mp.info.4	Firma electrónica	n.a. ()
	mp.info.5	Sellos de tiempo	n.a. ()
	mp.info.6	Limpieza de documentos	L4
	mp.info.9	Copias de seguridad	L4
mp.s	Protección de los servicios		
	mp.s.1	Protección del correo electrónico (e-mail)	n.a. (_-L3)
	mp.s.2	Protección de servicios y aplicaciones web	L5
	mp.s.8	Protección frente a la denegación de servicio	L5
	mp.s.9	Medios alternativos	L5