Agencia Estatal
de Seguridad Aérea

Guía para la solicitud de derogación al Reglamento (UE) 2023/203 (Part IS) en AeMCs

GOBIERNO DE ESPAÑA
MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

REGISTRO DE EDICIONES		
EDICIÓN	**Fecha de APLICABILIDAD**	**MOTIVO DE LA EDICIÓN DEL DOCUMENTO**
01	Desde publicación	Primera Edición

REFERENCIAS	
CÓDIGO	**TÍTULO**
LEY 39/2015	LEY 39/2015, DE 1 DE OCTUBRE, DEL PROCEDIMIENTO ADMINISTRATIVO COMÚN DE LAS ADMINISTRACIONES PÚBLICAS
LEY 21/2003	LEY 21/2003, DE SEGURIDAD AÉREA
REAL DECRETO 98/2009	REAL DECRETO 98/2009, DE 6 DE FEBRERO, POR EL QUE SE APRUEBA EL REGLAMENTO DE INSPECCIÓN AÉREA
REGLAMENTO (UE) 2018/1139	REGLAMENTO (UE) 2018/1139 DEL PARLAMENTO EUROPEO Y DEL CONSEJO DE 4 DE JULIO DE 2018 SOBRE NORMAS COMUNES EN EL ÁMBITO DE LA AVIACIÓN CIVIL Y POR EL QUE SE CREA UNA AGENCIA DE LA UNIÓN EUROPEA PARA LA SEGURIDAD AÉREA Y POR EL QUE SE MODIFICAN LOS REGLAMENTOS (CE) Nº 2111/2005, (CE) Nº 1008/2008, (UE) Nº 996/2010, (CE) Nº 376/2014 Y LAS DIRECTIVAS 2014/30/UE Y 2014/53/UE DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y SE DEROGAN LOS REGLAMENTOS (CE) Nº 552/2004 Y (CE) Nº 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO Y EL REGLAMENTO (CEE) Nº 3922/91 DEL CONSEJO.
REGLAMENTO (UE) Nº 1178/2011	REGLAMENTO (UE) Nº 1178/2011 DE LA COMISIÓN, DE 3 DE NOVIEMBRE DE 2011, POR EL QUE SE ESTABLECEN REQUISITOS TÉCNICOS Y PROCEDIMIENTOS ADMINISTRATIVOS RELACIONADOS CON EL PERSONAL DE VUELO DE LA AVIACIÓN CIVIL EN VIRTUD DEL REGLAMENTO (CE) Nº 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO.
REGLAMENTO (UE) 2015/340	REGLAMENTO (UE) 2015/340 DE LA COMISIÓN DE 20 DE FEBRERO DE 2015 POR EL QUE SE ESTABLECEN REQUISITOS TÉCNICOS Y PROCEDIMIENTOS ADMINISTRATIVOS RELATIVOS A LAS LICENCIAS Y LOS CERTIFICADOS DE LOS CONTROLADORES DE TRÁNSITO AÉREO EN VIRTUD DEL REGLAMENTO (CE) Nº 216/2008 DEL PARLAMENTO EUROPEO Y DEL CONSEJO, SE MODIFICA EL REGLAMENTO DE EJECUCIÓN (UE) Nº 923/2012 DE LA COMISIÓN Y SE DEROGA EL REGLAMENTO (UE) Nº 805/2011 DE LA COMISIÓN
REGLAMENTO (UE) 2023/203	REGLAMENTO DE EJECUCIÓN (UE) 2023/203 DE LA COMISIÓN, DE 27 DE OCTUBRE DE 2022, POR EL QUE SE ESTABLECEN DISPOSICIONES DE APLICACIÓN DEL REGLAMENTO (UE) 2018/1139 DEL PARLAMENTO EUROPEO Y DEL CONSEJO EN LO QUE SE REFIERE A LOS REQUISITOS RELATIVOS A LA GESTIÓN DE LOS RIESGOS RELACIONADOS CON LA SEGURIDAD DE LA INFORMACIÓN QUE PUEDAN REPERCUTIR SOBRE LA SEGURIDAD AÉREA

LISTADO DE ACRÓNIMOS	
ACRÓNIMO	**DESCRIPCIÓN**
AEMC	CENTRO MÉDICO EXAMINADOR AÉREO
AME	MÉDICO EXAMINADOR AÉREO
MED	REQUISITOS MÉDICOS
UE	UNIÓN EUROPEA

ÍNDICE

1. INTRODUCCIÓN

Esta Guía tiene por objeto definir el proceso a seguir por las organizaciones vinculadas al ámbito de la Medicina Aeronáutica para solicitar a AESA la aprobación de la derogación de algunos de los requisitos establecidos por la Part IS, de acuerdo con lo establecido por el IS.I.OR.200 (e).

2. OBJETO Y ALCANCE

El *Reglamento de Ejecución (UE) 2023/203 de la Comisión, de 27 de octubre de 2022, por el que se establecen disposiciones de aplicación del Reglamento (UE) 2018/1139 del Parlamento Europeo y del Consejo en lo que se refiere a los requisitos relativos a la gestión de los riesgos relacionados con la seguridad de la información que puedan repercutir sobre la seguridad aérea,* otorga a la autoridad competente, por medio del IS.I.OR.200 (e), la posibilidad de eximir a una organización de la aplicación de los requisitos establecidos en las letras (a) a (d) del requisito IS.I.OR.200, así como en los puntos IS.I.OR.205 a IS.I.OR.260, si se demuestra a satisfacción de AESA que las actividades, instalaciones y recursos, así como los servicios que presta, recibe y mantiene la organización, no plantean un riesgo para la seguridad de la información con un impacto potencial en la seguridad aérea, ni para sí misma ni para otra organización. Todo ello, sin perjuicio de la obligación de cumplir los requisitos de información establecidos en el Reglamento (UE) nº 376/2014 y los requisitos establecidos en IS.I.OR.200 (a)(13) relativo a la protección de la confidencialidad de la información recibida de otras organizaciones, en función de su nivel de sensibilidad.

Es por ello que se pretenden definir, por medio de esta guía, los criterios para facilitar el proceso de solicitud de derogación de estos requisitos a aquellos Centros de Medicina Aeronáutica interesados en este fin.

La aprobación de la derogación se basará en una Evaluación Documentada de los Riesgos para la Seguridad de la Información, que deberá ser realizada por la organización o por un tercero de conformidad con el punto IS.I.OR.205, y ser revisada y aprobada por AESA.

Esta evaluación de riesgos puede llevarse a cabo y documentarse utilizando el procedimiento de evaluación de riesgos existente en la organización, o bien un procedimiento definido ad hoc para los riesgos de seguridad de la información con efecto en la seguridad operacional.

3. DEFINICIONES

Serán de aplicación los conceptos de las referencias normativas indicadas en la sección REFERENCIAS.

4. PROCEDIMIENTO DE DEROGACIONES A LA PARTE IS

4.1. Proceso de solicitud de derogación del AeMC

La solicitud de derogación del cumplimiento de los correspondientes requisitos de la Parte IS podrá realizarse de las formas descritas a continuación:

- Si la organización ya dispone de Certificado de AEMC autorizado, realizando la solicitud a través del procedimiento electrónico de Solicitud General de la Sede Electrónica de AESA, aportando:

  1. Solicitud de derogación de acuerdo al formato MED-AeMC-P01-F14, firmada por el Gerente responsable

  2. Evaluación de riesgos de seguridad de la información individualizada y específica del Centro que lo solicita, pudiendo tomar como punto de partida el material guía propuesto en el "Anexo II. Material guía para el desarrollo de la evaluación de riesgos de seguridad de la información.

  del presente documento.

- Si la organización está en vía de solicitud de Certificado de AEMC autorizado, realizando la solicitud en el marco del correspondiente proceso de certificación como AeMC, indicando en el formulario de solicitud MED-AeMC-P01-F01, su intención de solicitar la correspondiente derogación.

  Asimismo, se deberá aportar la correspondiente evaluación de riesgos de seguridad de la información individualizada y específica del Centro que lo solicita, pudiendo tomar como punto de partida, igualmente, el material guía propuesto en el "Anexo II. Material guía para el desarrollo de la evaluación de riesgos de seguridad de la información.

  del presente documento.

4.1.1. Proceso de elaboración de la Evaluación Documentada de los Riesgos para la Seguridad de la Información

Se sugiere tener en cuenta las siguientes consideraciones previas a la realización de la evaluación documentada de los riesgos de seguridad de la información que acompañe la solicitud de derogación:

- La organización podrá utilizar la metodología de evaluación de riesgos ya establecida como parte obligatoria de su Sistema de Gestión de Seguridad para abordar los riesgos para la seguridad de la información; o, en su defecto, podrá realizar la evaluación de riesgos de

seguridad de la información basándose en la metodología descrita en la sección 4.1.1.1, o cualquier otra metodología adecuada para este fin.

- La metodología deberá ser aplicada por personal que tenga conocimientos sobre su uso, según se define en el IS.I.OR.240. La organización deberá disponer de personal con conocimientos suficientes en ciberseguridad (o recurrir a personal externo/subcontratado experto), y deberá asegurar el conocimiento básico en la materia por parte del Gerente Responsable.
- El Manual de Gestión del AeMC deberá ser aprobado por AESA tras acreditar que se da garantía del desarrollo de los procedimientos que el centro propone desempeñar para dar cumplimiento a los requisitos IS.I.OR.200(a)(13) (no derogable), IS.I.OR.205(d) y IS.I.OR.240(3).

En definitiva, la organización deberá especificar tanto la metodología utilizada para realizar la evaluación de riesgos para la seguridad de la información, como el listado de personas (tanto pertenecientes a la organización como externas a ella) y funciones implicadas en el proceso de evaluación de riesgos para la seguridad de la información.

Una vez concretado lo anterior, en la evaluación de riesgos se identificarán los riesgos para la seguridad de la información que puedan tener un impacto potencial en la seguridad aérea, teniendo presentes los siguientes aspectos:

- Tamaño y complejidad de la organización.
- Impacto potencial en la seguridad causado por incidentes de seguridad de la información, en los servicios que presta y recibe la organización, incluidas sus interfaces.
- Procesos que la organización ha establecido para prestar y recibir los servicios.
- Posición de la organización dentro de la cadena funcional de la aviación y el consiguiente grado de criticidad de la organización dentro del ámbito de la aviación civil en el Estado miembro.
- Actividades transfronterizas de la organización, si procede.
- Madurez del sistema de gestión de la seguridad de la organización, si procede.
- Listado de sistemas digitales, flujos de datos y procesos.

4.1.1.1 Metodología para la Evaluación Documentada de los Riesgos para la Seguridad de la Información

La metodología aplicada para este proceso deberá incluir los aspectos descritos por el IS.OR.205:

1. (IS.OR.205(a)) Identificación de todos los elementos que pueden estar expuestos a riesgos de seguridad de la información, incluyendo: actividades, instalaciones y recursos, así como los servicios que opera, proporciona, recibe o mantiene; equipos, sistemas, datos e información que contribuyan al funcionamiento de los elementos anteriores.

2. (IS.OR.205(b)) Identificación de las interfaces y flujos de datos con otras organizaciones

que puedan suponer, tanto como para la propia organización como para las externas, la exposición a riesgos de seguridad de la información que puedan incrementar los riesgos de seguridad operacional aérea.

3. (IS.OR.205(c)) Definir una metodología de evaluación y clasificación de los riesgos identificados, con el fin de poder determinar el nivel de aceptación o mitigación de cada uno de ellos. Esto implica que, para cada riesgo identificado, se aplique lo siguiente:

   - Asignación de un nivel de riesgo según la clasificación que haya sido predefinida, teniendo en cuenta la probabilidad de ocurrencia y la severidad de sus consecuencias, identificando asimismo la repercusión del mismo sobre la seguridad aérea
   - Clasificación del riesgo en base a los criterios de aceptación del riesgo establecidos. Es decir, deberá ser aceptado o mitigado de acuerdo con el criterio que defina la organización para todos aquellos que tengan un potencial impacto en la seguridad operacional aérea.

   Para esto, se podrá considerar la opción de aplicar la misma metodología de evaluación de riesgos que la organización tenga implantada dentro de su Sistema de Gestión de la Seguridad Operacional, adaptándola a las particularidades de los Sistemas de Seguridad de la Información.

Esta evaluación de riesgos de seguridad de la información deberá ser un proceso riguroso y documentado que deberá ser periódicamente revisado y actualizado, conforme a lo que establece el IS.OR.205(d).

4.1.1.2 Mantenimiento de los requisitos para la derogación

El AeMC conservará la aprobación de la derogación siempre y cuando se sigan cumpliendo con los criterios y condiciones por los que se otorgó y no se renuncie a ella o haya sido revocada.

Por ello, la organización deberá mantener evidencia documentada de la metodología utilizada, registro de riesgos y trazabilidad del correspondiente proceso de análisis y clasificación de los mismos, y la justificación de la aceptabilidad del riesgo y la no repercusión de los mismos sobre la seguridad aérea; así como monitorizar e informar a AESA de los cambios que puedan producirse en su Evaluación Documentada de los Riesgos para la Seguridad de la Información y/o en el alcance de sus actividades.

El cumplimiento con los criterios y condiciones por los que se otorgaron la derogación serán revisados por AESA en el marco de los Planes de Vigilancia Continuada aplicables a la organización.

5. CAMBIOS RELEVANTES DE ESTA EDICIÓN

Primera edición del documento.

6. ANEXOS

Anexo I. Proforma de procedimientos a incorporar en el Manual de Gestión para dar cumplimiento a los elementos no derogables de la Part IS.

Anexo II. Material guía para el desarrollo de la evaluación de riesgos de seguridad de la información.

ANEXO I. PROFORMA DE PROCEDIMIENTOS A INCORPORAR EN EL MANUAL DE GESTIÓN PARA DAR CUMPLIMIENTO A LOS ELEMENTOS NO DEROGABLES DE LA PART IS.

El presente Anexo describe una proforma orientativa del contenido que deberá añadir el AeMC en su Manual de Gestión para poder completar la solicitud de aprobación derogación al Reglamento (UE) 2023/203 (Part IS) en AeMCs, teniendo en cuenta los elementos no derogables del mismo.

PROCEDIMIENTOS PARA LOS ELEMENTOS NO DEROGABLES DE LA PART IS – MANUAL DE GESTIÓN

IS.I.OR.200 (a)(13) – Protección de Información recibida *(a incorporar como procedimiento del manual de gestión)*

Con el fin de dar cumplimiento al IS.OR.200 (a)(13), el AeMC establece en su Anexo X, un procedimiento para asegurar la protección de la información recibida de otras organizaciones. Este procedimiento contempla como elementos clave:

- Clasificación de la información recibida (confidencial, restringida, interna)
- Protección en tránsito (correo cifrado TSL, portales seguros)
- Protección en reposo (almacenamiento cifrado, control de accesos)
- Control de accesos
- Revisión anual de permisos y desactivación inmediata tras baja laboral

[Se deberá incluir en un Anexo al Manual el procedimiento que el Centro tiene implementado en términos de seguridad de la información para dar cumplimiento a lo anterior. Muchas de estas medidas de seguridad ya están implementadas en la actividad diaria del Centro y, en muchos casos, están además incluidas y detalladas en el Manual de Gestión].

Este procedimiento podrá estructurarse en base a los siguientes criterios:

- *Aplicabilidad:*

Este procedimiento aplica a toda información recibida por el AeMC en formato:

- electrónico
- papel
- documentación clínica o administrativa

- *Clasificación de la información*

Toda información recibida es clasificada en uno de los siguientes niveles:

Confidencial
Información sensible cuya divulgación no autorizada podría afectar a la seguridad operacional, cumplimiento normativo o privacidad médica.
Ejemplos: historiales médicos aeronáuticos, informes médicos, …

Restringida
Información destinada a uso interno limitado dentro del AeMC.
Ejemplos: informes de auditoría, comunicaciones profesionales.

Interna
Información de carácter operativo con bajo nivel de sensibilidad.

La clasificación es indicada/marcada como tal, cuando es posible, en el documento o sistema de almacenamiento.

- *Protección de la información en tránsito*

La información clasificada como confidencial o restringida deberá transmitirse mediante:

- correo electrónico protegido con cifrado TLS
- plataformas o portales seguros
- redes corporativas seguras o VPN

No está permitido transmitir información confidencial mediante:

- correos electrónicos personales
- aplicaciones de mensajería no autorizadas
- sistemas de almacenamiento externo no aprobados.

La documentación física (con laboratorio, candidatos al certificado **médico, comunicaciones con AESA…) se enviará en sobres cerrados y correctamente identificados (con laboratorio, candidatos al certificado médico, comunicaciones** con AESA…)

- *Protección de la información en reposo*
    a. Almacenamiento electrónico

    La información se almacenará únicamente en:

    - servidores o sistemas informáticos autorizados del AeMC
    - aplicaciones clínicas seguras
    - App SIGMA2 de AESA
    - repositorios con medidas de cifrado y control de acceso

    b. Documentación en papel

    Los documentos físicos deberán guardarse en:

    - archivadores cerrados con llave
    - zonas de acceso restringido al personal autorizado.

- *Control de accesos*

El acceso a la información recibida se limitará al personal que lo necesite para el desempeño de sus funciones, aplicando el principio de **"necesidad de conocer"**.

Se aplicarán las siguientes medidas:

- cuentas de usuario individuales
- autenticación mediante contraseña
- perfiles de acceso según función
- registro de accesos cuando sea posible

- *Revisión de accesos*

El responsable del AeMC o el responsable de seguridad de la información realizará:

- revisión anual de los permisos de acceso
- verificación de la necesidad de dichos accesos.

Los accesos deberán **desactivarse inmediatamente** en caso de:

- baja laboral
- finalización de contrato
- cambio de funciones.

- *Gestión de incidentes*

Cualquier incidente relacionado con:

- pérdida de información
- acceso no autorizado
- posible filtración de datos

deberá notificarse inmediatamente al responsable de seguridad del AeMC (haciendo partícipe al Director Médico) para su registro, evaluación y aplicación de medidas correctivas.

IS.I.OR.205(D) REEVALUACIÓN PERIÓDICA CUANDO CAMBIE EL ENTORNO *(a incorporar como procedimiento del manual de gestión)*

Conforme a lo establecido por el IS.I.OR.205(d), el AeMC revisará y actualizará la evaluación de riesgos realizada, siguiendo el procedimiento de evaluación de riesgos aprobado y predefinido, siempre que se den las siguientes situaciones:

(1) se produce un cambio en los elementos sujetos a riesgos de seguridad de la información;
(2) se produce un cambio en las interfaces entre la organización y otras organizaciones, o en los riesgos comunicados por las otras organizaciones;
(3) se produce un cambio en la información o los conocimientos utilizados para la identificación, el análisis y la clasificación de los riesgos;
(4) se extraen lecciones del análisis de los incidentes de seguridad de la información.

IS. I. OR. 240(3) PROCEDIMIENTO PARA LA DESIGNACIÓN DEL RESPONSABLE DE SEGURIDAD DE LA INFORMACIÓN *(a incorporar como procedimiento del manual de gestión)*

Este procedimiento aplica a la designación de al menos una persona dentro de la organización con comprensión del Part-IS, que actuará como punto de referencia interno para la seguridad de la información.

El responsable del AeMC designará formalmente al Responsable de Seguridad de la Información (RSI) conforme a los criterios de selección definidos por el AeMC, que deberán garantizar que el RSI propuesto:

1. Conoce el contenido fundamental del PART IS
2. Tiene conocimiento del alcance de la organización y sus obligaciones regulatorias, especialmente de los aspectos derogables y no derogables de la PART IS
3. Actuará como punto de contacto interno y externo, incluyendo las comunicaciones con la Autoridad Competente
4. Participará en la evaluación de riesgos de seguridad de la información
5. supervisará la aplicación de las medidas mínimas de protección de información.

Entre los criterios de selección se incluirán, como mínimo:

- Acreditación de la formación del RSI en Part IS, formación en ciberseguridad básica o seguridad de la información, o evidencia documental de que recibirá formación adecuada tras su designación
- Responsabilidad del RSI definida en el Manual de Gestión: (mantener conocimiento básico de los requisitos de Part-IS; apoyar la identificación y evaluación de riesgos; supervisar el cumplimiento de las medidas de protección de información; actuar como punto de contacto con la Autoridad Competente cuando proceda; informar al responsable del AeMC de cualquier riesgo o incidente relevante…)
- Conocimiento y participación del RSI en la evaluación de riesgos
- Compromiso de mantener la supervisión mínima continua de los requisitos derogados y no derogados de la PART IS

Una vez designado por el AeMC, se presentará previa solicitud de cambio a AESA para su aprobación, la justificación documental de que el candidato cumple con los requisitos anteriores.

Así, el centro conservará como registro documental:

- Documento de designación del RSI
- Descripción de responsabilidades del RSI
- Evidencia de formación del RSI
- Participación del RSI en evaluaciones de riesgos.

La designación del Responsable de Seguridad de la Información se revisará al menos una vez al año, o cuando cambie la estructura organizativa o la persona designada.

ANEXO II. MATERIAL GUÍA PARA EL DESARROLLO DE LA EVALUACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN.

El presente Anexo describe una proforma orientativa del contenido de la evaluación de riesgos particularizada que deberá incluir el AeMC como adjunto a su solicitud de aprobación derogación al Reglamento (UE) 2023/203 (Part IS) en AeMCs.

EVALUACIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN

Se deberá aportar como documento independiente junto con el resto de documentación requerida en la solicitud de derogación presentada.

La evaluación de riesgos desarrollada por el AeMC podrá seguir la siguiente estructura:

1. **Alcance**

1.1 Sistemas incluidos

- Sistema de gestión de historiales médicos aeronáuticos
- Canales de comunicación (comunicación con laboratorios subcontratados u otros agentes por medio de correo electrónico, mensajería, accesos remotos…)
- Uso de sistemas externos (aplicación SIGMA de AESA, aplicaciones de gestión, o aplicaciones de almacenamiento de uso interno…)
- Infraestructura informática interna: equipos, redes locales, almacenamiento digital/local/documental físico

1.2 Tipos de información

- Datos personales identificativos
- Datos médicos
- Informes de aptitud psicofísica
- Resultados de analíticas
- Documentación regulatoria
- Documentación interna

2. **Metodología**

Se debe detallar la metodología empleada para obtener la evaluación de riesgos.

Será recomendable utilizar la misma metodología de evaluación de riesgos que la organización tiene implantada dentro de su Sistema de Gestión de Seguridad, aunque esto implique, si precisa, una actualización o adaptación de la misma.

En su defecto, se deberá detallar la metodología a emplear por el AeMC para esta evaluación de riesgos, debiéndose documentar adecuadamente. Esta metodología deberá incluir:

2.1 Identificación de activos

Identificación de todos los elementos que pueden estar expuestos a riesgos de la seguridad de la información.

2.2 Evaluación de los riesgos identificados

Se evaluarán los riesgos asociados a cada activo, teniendo en cuenta la probabilidad de ocurrencia y la severidad de sus consecuencias, y considerando su repercusión sobre la seguridad aérea.

2.2.1 Asignación de la probabilidad de ocurrencia

Se tendrá en cuenta cuál es la probabilidad de que el evento identificado que afecta a la seguridad de la información pueda ocurrir de nuevo, o cuál es la probabilidad de que pueda ocurrir algo similar.

Nivel		
A	Muy improbable	Riesgo teórico que requiere de circunstancias muy excepcionales para materializarse. No existen casos documentados de que haya ocurrido.
B	Improbable	Rara probabilidad de que ocurra. Existen pocos casos documentados.
C	Posible	Poco probable. Es posible que ocurra, pero no se materializa de forma periódica.
D	Ocasional	Probabilidad de que ocurra periódicamente.
E	Frecuente	Ocurre constantemente, con bastante frecuencia.

2.2.2 Asignación del grado de severidad

Se tendrá en cuenta qué impacto tendría sobre la seguridad operacional, la materialización de la amenaza sobre la seguridad de la información.

Nivel		
1	Insignificante	Sin impacto en la seguridad operacional. Sin impacto en la actividad del AeMC. Fallo puntual sin pérdida de datos ni impacto en sistemas críticos.
2	Menor	Sin impacto directo en la seguridad operacional. Supone la interrupción temporal de los servicios prestados por el centro, o retrasos por la indisponibilidad parcial de herramientas no críticas (correo, sistema de citas de pacientes…). No supone la pérdida de datos médicos.
3	Moderado	Impacto potencial indirecto; puede comprometer el nivel de seguridad operacional. Implica retrasos en la emisión de certificados, cancelación de consultas programadas. Supone posible pérdida de datos no críticos o necesidad de reprocesar la información.
4	Grave	Compromete la seguridad operacional. Interrupción o cancelación significativa de reconocimientos médicos. Caída de sistemas críticos (historia clínica, certificados, bases de datos…) sin recuperación inmediata. Supone la pérdida de la integridad y disponibilidad de los registros médicos. Pérdida o corrupción de datos médicos relevantes.
5	Catastrófico	Riesgo grave para la seguridad de vuelo (Certificados incorrectos o no verificables). Paralización total prolongada de la actividad del AeMC por la imposibilidad de acceder a la documentación de carácter sensible o critica, sin respaldo funcional. Pérdida irreversible de historiales médicos.

2.3 Clasificación de los riesgos identificados

Habiendo sido evaluadas las variables de probabilidad y severidad del riesgo asociado (Probabilidad x Severidad), se procederá a clasificar el mismo utilizando como herramienta la siguiente matriz de riesgos.

	Catastrófico (5)	Graves (4)	Moderado (3)	Menor (2)	Insignificante (1)
Frecuente (E)	E5 (Alto)	E4 (Alto)	E3 (Alto)	E2 (Medio)	E1 (Medio)
Ocasional (D)	D5 (Alto)	D4 (Alto)	D3 (Medio)	D2 (Medio)	D1 (Medio)
Posible (C)	C5 (Alto)	C4 (Medio)	C3 (Medio)	C2 (Medio)	C1 (Aceptable)
Improbable (B)	B5 (Medio)	B4 (Medio)	B3 (Medio)	B2 (Aceptable)	B1 (Aceptable)
Muy improbable (A)	A5 (Medio)	A4 (Medio)	A3 (Aceptable)	A2 (Aceptable)	A1 (Aceptable)

Esto dará lugar a 3 tipos de riesgos: críticos, revisables y aceptables. Estos serán aceptados o mitigados, de acuerdo con el criterio establecido a continuación:

Clasificación	Criterio de gestión del riesgo
Crítico:	El riesgo es inaceptable y es necesario implementar medidas de mitigación.
Revisable:	Se necesitan medidas de mitigación para reducir el riesgo a un nivel aceptable. Si no resulta práctico o viable mitigar o reducir el riesgo, se podrá aceptar siempre que se mantenga bajo supervisión periódica.
Aceptable:	Riesgo aceptable. Sujeto a revisión periódica.

Con el fin de poder solicitar y mantener la aprobación de derogación conforme a lo establecido por el IS.I.OR.200(e), el AeMC se asegurará de gestionar sus riesgos de tal forma que garantice que se mantienen en un nivel aceptable y que, por tanto, no suponen un impacto potencial en la seguridad aérea.

3. Evaluación de riesgos del AeMC

Se deberá incluir la evaluación de riesgos particularizada e individualizada para el AeMC, conforme a la metodología que anteriormente haya sido definida y elegida.

3.1 Identificación de activos. Vulnerabilidades y amenazas asociadas *(a particularizar por cada AeMC)*

ACTIVO	Descripción	Amenazas/Vulnerabilidades
Aplicación SIGMA AESA	Plataforma de gestión de expedientes	Acceso no autorizado a la app de AESA Malware /ransomware Caída del sistema AESA Fallos de conexión
Historiales médicos y datos personales	Datos clínicos completos y datos identificativos o personales	Gestión deficiente o ausencia de control accesos Posible almacenamiento local sin cifrado
Comunicaciones con laboratorio u otras organizaciones	Resultados y solicitudes	Intercepción de datos enviados al laboratorio Envío de información a destinatario incorrecto Uso de canales no seguros (email sin cifrar) Falta de control sobre proveedores (laboratorio)

		Ausencia de procedimientos formales Subcontratación sin cláusulas de seguridad
Infraestructura IT	PCs, red almacenamiento digital, plataforma de programación de citas	Perdida de dispositivos portátiles, USB Posible almacenamiento local sin cifrado Ausencia de control accesos a los dispositivos Malware /ransomware Fallos de conexión de plataformas de gestión de citas
Personal	Personal médico y administrativos	Errores del personal (envíos incorrectos) Uso indebido de credenciales Falta de formación en seguridad de la información Ausencia de procedimientos formales Uso de email sin cifrado para datos médicos
Documentación física	Registros/formularios impresos	Gestión deficiente o ausencia de control accesos Ausencia de procedimientos formales Posible almacenamiento local sin cifrado

3.2 Análisis de riesgos *(a particularizar por cada AeMC)*

Escala	
Probabilidad	• Muy improbable • Improbable • Posible • Ocasional • Frecuente
Impacto	• Insignificante • Menor • Moderado • Grave • Catastrófico
Nivel	• Alto • Medio • Bajo

RIESGO	Probabilidad	Impacto	Nivel (Prob. X Impacto)	Medidas de mitigación	Riesgo residual
(1) Ciberataque/ Malware/ransomware en los equipos o dispositivos locales, en bases de datos o plataformas propias del AeMC	Posible (C)	Grave (4)	(C4)	Antivirus Actualizaciones de software y parches de seguridad Copias de seguridad periódicas Segmentación de red Uso de canales seguros (TLS, VPN…) Gestión de registros y expedientes por medio de la aplicación de AESA (subida de registros y emisión de certificados mediante aplicación AESA) Cifrado de datos críticos o sensibles almacenados fuera de la aplicación de AESA	Aceptable (A3)
(2) Acceso no autorizado a la app de AESA	Posible (C)	Grave (4)	(C4)	Autenticación fuerte (multifactor) Gestión de usuarios por roles Revisión periódica de accesos Tramitación inmediata de altas/bajas de usuarios Procedimiento de suspensión o bloqueo de equipos si el autorizado abandona su puesto	Aceptable (A3)
(3) Caída de la plataforma o sistema de citas	Posible (C)	Menor (2)	(C2)	Sistema alternativo manual de programación de citas Soporte IT propio del AeMC o subcontratado	(C1)(B2) Aceptable
(4) Incidencias de conexión a red que impide acceso a aplicación de gestión de expedientes	Posible (C)	Menor (2)	(C2)	Soporte IT propio del AeMC o subcontratado	(C1)(B2) Aceptable
(5) Caída del sistema AESA	Posible (C)	Moderado (3)	(C3)	Procedimiento de notificación de incidentes inmediata con AESA y con soporte IT Procedimientos y medidas de recuperación de AESA	(B2) Aceptable
(6) Acceso no autorizado a datos clínicos o registros completos en carpetas de dispositivos locales /	Improbable (B)	Grave (4)	(B3)	Contraseñas fuertes Autenticación multifactor Gestión de usuarios por roles Revisión periódica de accesos Tramitación inmediata de altas/bajas de usuarios	(A3) (B2) Aceptable

carpetas en red / archivo físico				Armarios con cerraduras/candados y permisos de acceso limitado Gestión de registros y expedientes por medio de la aplicación de AESA (subida de registros y emisión de certificados mediante aplicación AESA)	
(7) Intercepción de datos enviados al laboratorio	Improbable (B)	Grave (4)	(B4)	Uso de canales seguros (TLS, email cifrado, plataformas seguras…) Contrato con cláusulas de seguridad Verificación de destinatarios Gestión de registros y expedientes por medio de la aplicación de AESA (subida de registros y emisión de certificados mediante aplicación AESA)	(A3) (B2) Aceptable
(8) Envío erróneo de resultados / Envío de información a destinatario incorrecto	Improbable (B)	Grave (4)	(B4)	Verificación de destinatarios Formación periódica al personal Procedimiento de notificación de incidentes Procedimientos claros de envío de datos sensibles mediante correos cifrados y del manejo de datos	(A3) Aceptable
(9) Pérdida de dispositivos portátiles, USB	Improbable (B)	Grave (4)	(B4)	Contrato con cláusulas de seguridad con el personal del AeMC Dispositivos cifrados con contraseñas fuertes Gestión de registros y expedientes por medio de la aplicación de AESA (subida de registros y emisión de certificados mediante aplicación AESA)	(A3) (B2) Aceptable
…	…	…	…	…	…

4. Conclusiones

Se deberán incluir las conclusiones que se extraigan de la evaluación de riesgos, detallando que los resultados obtenidos (riesgos mitigados y no impacto sobre la seguridad operacional) justifican la solicitud de derogación de la Part IS.