WEBINAR CAMO/145 PARTE-IS

Nº	PREGUNTAS ORGANIZACIONES	RESPUESTA AESA* *Las respuestas recogidas en este documento tienen carácter orientativo y no son vinculantes.
1	**¿Se hará llegar a los participantes la presentación (PPT) utilizada durante la jornada?**	La presentación y el documento con las preguntas y respuestas tratadas durante el Webinar están disponibles en la página web de AESA, en el apartado: https://www.seguridadaerea.gob.es/ambitos/aeronaves/aeronavegabilidad-continuada/actividades-con-el-sector
2	**En caso de que, llegada la fecha de febrero de 2026, el MOE adaptado a los requisitos de la Parte-IS aún no estuviera aprobado, ¿podría verse afectada la aprobación de la organización?**	Si la organización está dentro del ámbito de aplicación de la Parte-IS, no ha obtenido una derogación y los cambios requeridos en el MOE no han sido aprobados antes del 22/02/2026, se considerará una situación de incumplimiento normativo. En dicho escenario, las medidas a adoptar dependerán del alcance de la aprobación de la organización y del grado de exposición a riesgos en materia de Seguridad de la Información. AESA evaluará cada caso de manera individualizada, analizando los procedimientos implantados y la situación real de la organización. Como resultado de dicha evaluación, podría determinarse la emisión de una no conformidad de nivel 1 o 2 y, en su caso, la aplicación de limitaciones a la aprobación de la organización. AESA recomienda presentar la solicitud de aprobación de los cambios a la mayor brevedad posible, con el fin de disponer del tiempo necesario para su evaluación y para la resolución de posibles no conformidades. Se agradecería que las solicitudes se presentaran antes de final de año.

PASEO DE LA CASTELLANA 112
28046 MADRID
TEL.: +34 91 396 8000

3	**En relación con la Parte-IS, ¿quién será responsable de la aprobación? ¿La Oficina de Supervisión de Vuelo (OSV) o los Servicios Centrales?**	La evaluación y aprobación de los cambios necesarios para la implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) será realizada por la unidad de supervisión responsable de la aprobación de la organización. Dicha supervisión podrá ser ejercida por la correspondiente Oficina de Supervisión de Vuelo (OSV) o, en su caso, por la División de Aprobaciones y Estandarización de Aeronavegabilidad, dependiendo de la asignación establecida.
4	**En el caso de un grupo empresarial (holding) que incluye varias organizaciones CAMO, ¿sería posible elaborar un único manual que abarque a todas ellas, reflejando sus particularidades?**	En organizaciones que formen parte de un mismo grupo empresarial, es posible optar por diferentes enfoques en relación con el Sistema de Gestión de la Seguridad de la Información (SGSI). Cada organización puede disponer de un SGSI individual o, alternativamente, se puede desarrollar un SGSI global a nivel de grupo, siempre que cada organización/aprobación haga referencia explícita a dicho SGSI global en su documentación y se reflejen adecuadamente las particularidades o diferencias aplicables a cada una.
5	**Si se opta por implantar un SGSI común para las organizaciones del grupo con aprobaciones AOC/CAMO/Parte-145, ¿cómo debe realizarse la presentación de la documentación y a qué unidad de AESA debe dirigirse para su evaluación y aprobación?**	AESA permite la implantación de un SGSI común para varias aprobaciones dentro de un mismo grupo (AOC, CAMO y Parte-145), siempre que se desarrollen los procedimientos correspondientes en un Manual del Sistema de Gestión de la Seguridad de la Información común. En el caso de organizaciones con aprobación AOC, la solicitud de aprobación de cambios deberá remitirse a la Unidad de Supervisión de Operaciones asignada, dirigida a la atención del Principal de Operaciones. La evaluación de estos cambios se llevará a cabo siguiendo el mismo procedimiento actualmente aplicable para los cambios en sistemas de gestión comunes dentro de una misma organización con múltiples aprobaciones.
6	**¿Se conoce la fecha prevista para la actualización del Reglamento (UE) 376/2014 que incluirá los sucesos relacionados con la Parte-IS?**	Por el momento, no existe una fecha prevista para la actualización del Reglamento (UE) 376/2014 que incorpore los sucesos vinculados a la Parte-IS.
7	**En relación con la solicitud de derogación, cuando se indica que debe incluirse en la memoria de la organización una referencia al ISMS (SGSI), ¿en qué apartados y de qué**	En el caso de una solicitud de derogación, no es necesario incluir una descripción del Sistema de Gestión de la Seguridad de la Información (SGSI/ISMS) en la memoria, dado que dicho sistema no existiría si la derogación es concedida.

	manera debe incorporarse dicha información?	No obstante, la memoria debe reflejar y desarrollar aquellos apartados en los que la Parte-IS tiene implicación, incluso en situación de derogación, de acuerdo con los requisitos aplicables (por ejemplo, IS.I.OR.200(a)(13), IS.I.OR.240 o IS.I.OR.205). En función de la estructura documental de la organización, el requisito IS.I.OR.205 podrá estar incluido en la propia memoria o en un documento separado, como parte del Manual del Sistema de Gestión (MSG). Asimismo, en los manuales específicos —tales como la Parte 2 (CAME) o la Parte 3 (MOE)— podrá incluirse una referencia a la inexistencia del SGSI derivada de la derogación concedida, cuando proceda. La extensión y ubicación de estas referencias podrá variar en función de la redacción del documento y la estructura de la organización, pudiendo ser necesario reflejar menciones adicionales en otros apartados si corresponde.
8	**Para la aprobación inicial del SGSI, además del Manual del Sistema de Gestión de la Seguridad de la Información (MSGSI), ¿qué documentación debe presentarse? En caso de requerirse un análisis de riesgos inicial, ¿qué elementos mínimos debe incluir?**	Para la aprobación inicial del SGSI, no se establecen requisitos mínimos predeterminados respecto al contenido del análisis de riesgos. Corresponde a cada organización determinar el nivel de detalle necesario en función de su estructura, tamaño, complejidad y exposición a riesgos relacionados con la Seguridad de la Información. La organización deberá: - Identificar los peligros y amenazas vinculados a la Seguridad de la Información que puedan afectarle. - Evaluar los riesgos derivados de dichos peligros. - Definir e implementar medidas de mitigación o control, conforme a los procedimientos establecidos en su SGSI. El análisis de riesgos deberá estar alineado con los procesos definidos en el SGSI y permitir demostrar que la organización gestiona adecuadamente los riesgos relacionados con la Seguridad de la Información.

9	**Según una guía de EASA, tenía entendido que la solicitud de derogación no constituía un "Cambio Significativo". ¿Podrían aclararlo?**	En el ámbito de la aeronavegabilidad continuada, aplicable a las organizaciones con aprobación Parte-CAMO y/o Parte-145, no existe el concepto de "Cambio Significativo" tal y como se define en otros marcos normativos. La introducción de un Sistema de Gestión de la Seguridad de la Información (SGSI) en estas organizaciones se considera un cambio que requiere aprobación previa por parte de la autoridad, con independencia de que se solicite o no una derogación.
10	**¿Qué tipo de formación en materia de Parte-IS se espera que realicen las organizaciones? ¿Está dirigida únicamente al personal responsable del cumplimiento?**	La letra (f) del requisito IS.I.OR.240 establece que la organización debe disponer de personal suficiente para llevar a cabo las actividades relacionadas con la Parte-IS. Asimismo, la letra (g) exige que dicho personal posea la competencia necesaria para desempeñar sus funciones. Por tanto, no se define un único perfil ni un alcance específico de formación, ya que este dependerá de cómo la organización haya estructurado su implementación de la Parte-IS y de las funciones asignadas dentro de su SGSI. La organización deberá asegurarse de que todo el personal involucrado en actividades relacionadas con la Seguridad de la Información reciba la formación adecuada y sea competente para ejercer sus responsabilidades.
11	**¿Es obligatorio que el personal del ámbito Safety reciba formación en materia de ciberseguridad relacionada con la Parte-IS?**	No necesariamente. La formación en materia de ciberseguridad deberá impartirse únicamente al personal cuyas funciones estén relacionadas con la Seguridad de la Información, de acuerdo con lo establecido en el requisito IS.I.OR.240. Esto incluye, por ejemplo: - Personal que participe en procesos o actividades identificadas en la evaluación de riesgos como susceptibles de exposición a amenazas relacionadas con la Seguridad de la Información. - Personal que audite o supervise aspectos del SGSI y requiera dicho conocimiento para el desempeño de sus funciones. En resumen, deberá recibir formación aquel personal cuyas tareas requieran conocimientos en ciberseguridad en el marco del SGSI.

12	**En una organización certificada bajo la norma ISO 27001, si durante el análisis de riesgos específico del ámbito aeronáutico se concluye que no existen riesgos adicionales a los ya identificados mediante la ISO, ¿qué implicaciones tendría en relación con la Parte-IS?**	El hecho de que el análisis de riesgos específico del ámbito aeronáutico no identifique riesgos adicionales a los ya contemplados en la ISO 27001 no implica la ausencia de riesgos relacionados con la Seguridad de la Información. Simplemente indica que dichos riesgos ya están siendo gestionados dentro del Sistema de Gestión de Seguridad de la Información conforme a la ISO 27001. En este caso, la organización estaría cumpliendo los requisitos en materia de identificación y gestión de riesgos, lo que supone un ejemplo de integración natural entre la ISO 27001 y la Parte-IS. Por tanto, sería de aplicación la Parte-IS, al estar cubiertos los requisitos exigidos mediante el SGSI existente.
13	**¿Es obligatorio elaborar un Manual específico del Sistema de Gestión de la Seguridad de la Información (MSGSI), o es posible integrar su contenido dentro del MOE en el caso de organizaciones Parte-145?**	AESA no exige un manual independiente para el SGSI. La organización puede desarrollar los procedimientos del Sistema de Gestión de la Seguridad de la Información dentro del Manual del Sistema de Gestión, junto con los procedimientos del Sistema de Gestión de la Seguridad Operacional. Si la organización ha decidido integrar los procedimientos del Sistema de Gestión en el MOE, puede igualmente incorporar en dicho manual los procedimientos del SGSI, siempre que se garantice la trazabilidad y el cumplimiento de los requisitos aplicables de la Parte-IS.
14	**¿En qué casos es obligatorio designar una Persona Responsable Común (CRP)? La Guía de AESA indica "en los casos en que exista". En organizaciones pequeñas con aprobaciones AOC y CAMO y un mismo Director Responsable (DR), ¿sería obligatorio designar un CRP?**	La designación de una Persona Responsable Común (CRP) solo será necesaria cuando una organización disponga de varias aprobaciones y se determine que esta función debe ser asumida por una persona distinta del Director Responsable (DR). En el caso de una organización que cuente con aprobaciones AOC y CAMO y disponga de un único Director Responsable común (lo que ya es un requisito reglamentario), no existe obligación de designar un CRP adicional, siempre que las funciones y responsabilidades asociadas a dicha figura sean asumidas por el DR común.
15	**¿Está previsto unificar los requisitos de la Parte-IS con los establecidos en la SA-16 del Programa Nacional de Seguridad (PNS)?**	Los requisitos de la Parte-IS y los de la SA-16 del Programa Nacional de Seguridad estarán alineados en su enfoque y objetivos, pero no se unificarán, dado que se trata de marcos normativos distintos, cada uno con un ámbito de aplicación específico.
16	**¿Sería válido centralizar la relación entre Seguridad de la Información y Seguridad Operacional, de modo que esta última actúe**	La posibilidad de centralizar la relación entre la Seguridad de la Información y la Seguridad Operacional podrá evaluarse en función de la estructura organizativa, la asignación de responsabilidades y los recursos disponibles en cada organización.

	como punto focal con otras áreas como CAMO y Parte-145?	El Sistema de Gestión de Seguridad Operacional (SMS) y el Sistema de Gestión de la Seguridad de la Información (SGSI) formarán parte del Sistema de Gestión de la organización, cuyo máximo responsable será el Director Responsable (DR). Por tanto, la centralización de funciones podrá aceptarse siempre que se demuestre que: - Se mantienen claramente definidas las responsabilidades, - Se garantiza la adecuada coordinación entre sistemas, y - Se preserva la eficacia en la gestión tanto del SMS como del SGSI. La evaluación se realizará caso por caso.
17	**En el caso de que la organización haya designado una Persona Responsable Común (CRP), ¿puede o debe dicha persona firmar la declaración incluida en el Manual del SGSI (MSGSI)?**	De acuerdo con lo establecido en IS.I.OR.250(a), la declaración incluida en el Manual del Sistema de Gestión de la Seguridad de la Información (MSGSI) deberá ser firmada por el Director Responsable (DR) y, cuando corresponda, por el Chief Executive Officer (CEO). Por tanto, aunque exista una Persona Responsable Común (CRP), la firma de esta declaración no puede ser delegada en el CRP, salvo que coincida con el DR o el CEO conforme a la estructura de la organización.
18	**En un grupo empresarial (holding) que dispone de dos aprobaciones AOC, y donde el SGSI implantado es común para todo el grupo, ¿es posible elaborar un único manual que dé cobertura a ambos AOC?**	Sí. En el caso de un grupo empresarial que disponga de varias aprobaciones, es posible que exista un SGSI común que dé cobertura a todas ellas. En ese contexto, la organización puede desarrollar un único Manual del SGSI siempre que cada aprobación haga referencia al mismo y se reflejen adecuadamente las particularidades aplicables a cada organización cuando corresponda.
19	**Si el SGSI es corporativo y común para varias aprobaciones (AOC, CAMO y Parte-145), ¿debe ser auditado íntegramente por cada uno de los Controles de la Conformidad de cada aprobación, o puede delegarse dicha**	Cuando la organización opta por implantar un SGSI corporativo común para varias aprobaciones, dicho sistema debe incluir un Control de Conformidad (CC) definido dentro del SGSI. En este caso, será el Control de Conformidad del SGSI corporativo el responsable de realizar las auditorías internas que den cobertura a todas las aprobaciones implicadas (AOC, CAMO y Parte-145), sin necesidad de duplicar auditorías por parte de cada CC individual.

	auditoría en el Control de Conformidad del AOC?	
20	**En nuestro proceso de gestión de cambios, las modificaciones del MSG no implican cambios en el MOE/CAME, puesto que, al operar como una única organización ("One BG"), los cambios se reflejan en el Manual de Organización (MO). ¿Podemos mantener este enfoque también para el MSGSI?**	En principio, es posible mantener el mismo enfoque, dado que la filosofía de gestión del MSG y del MSGSI es equivalente y ambos forman parte del Sistema de Gestión de la organización. No obstante, la confirmación final sobre si este planteamiento puede seguir aplicándose será objeto de evaluación por parte del personal auditor de AESA, quien verificará que la trazabilidad documental, la gestión de cambios y la conformidad con los requisitos de la Parte-IS quedan suficientemente garantizadas.
21	**¿Es necesario realizar una auditoría interna del SGSI antes del 22 de febrero de 2026?**	Sí. La implantación del Sistema de Gestión de la Seguridad de la Información (SGSI) debe tratarse como un cambio sujeto a aprobación previa por parte de la autoridad. Por tanto, la solicitud deberá ir acompañada de: - Una auditoría interna previa, que verifique la implantación del SGSI, y - Una gestión de riesgos adecuada, conforme a los procedimientos de la organización. Estos elementos son necesarios para demostrar que el SGSI está implementado de acuerdo con los requisitos de la Parte-IS antes de la fecha límite.
22	**En grupos empresariales con varias organizaciones, ¿puede la misma persona desempeñar simultáneamente las funciones de Responsable de la Seguridad de la Información (RSI/CISO) y de Persona Responsable Común (PRC)?**	Sí, es posible que la misma persona asuma las funciones de Responsable de la Seguridad de la Información (RSI/CISO) y de Persona Responsable Común (PRC). No obstante, su idoneidad deberá evaluarse en función del alcance, complejidad y estructura de la organización o del grupo empresarial, garantizando en todo caso que se mantienen la independencia necesaria, la adecuada asignación de responsabilidades y la disponibilidad de recursos para el correcto desempeño de ambas funciones.
23	**En relación con la conservación de registros, cuando se menciona "registros de los procesos clave", ¿se refiere a copias de seguridad o a registros de logs?**	Tal como se indicó durante el webinar, el término "registros de los procesos clave" hace referencia a lo establecido en IS.I.OR.245(a)(1)(iii), que remite al requisito IS.I.OR.200(d). Este requisito se refiere a los procesos, procedimientos, roles y responsabilidades asociados a la implantación del Sistema de Gestión de la Seguridad de la Información (SGSI). Por tanto, estos registros corresponden a la evidencia generada para la propia implementación del SGSI (por ejemplo: evidencia de evaluaciones de riesgos, resultados de auditorías internas, indicadores del

		SGSI, seguimiento de acciones correctivas, etc.). No se refiere a las copias de seguridad o registros de logs, que se encuentran regulados, en su caso, por los requisitos aplicables del Reglamento (UE) 1321/2014 u otras normativas específicas. Cada tipo de registro se conservará conforme a los requisitos establecidos en la normativa que le resulte aplicable.
24	**Si existe un SGSI común para dos aprobaciones AOC y cada una cuenta con un Director Responsable (DR) distinto, ¿es obligatorio designar una Persona Responsable Común (CRP)? En ese caso, ¿podría dicha función ser asumida por el CISO?**	Sí. Cuando varias aprobaciones comparten un mismo SGSI, deberá designarse una Persona Responsable Común (CRP) para garantizar la coordinación y supervisión del sistema entre las diferentes organizaciones implicadas. La función de CRP podrá ser asumida por el CISO, siempre que la organización determine que esta persona cuenta con la competencia, autoridad y recursos necesarios para desempeñar ambas funciones y asegurar el cumplimiento de los requisitos establecidos para la Parte-IS.
25	**¿Dónde se pueden consultar los requisitos de formación aplicables al perfil de Responsable de Seguridad de la Información (CISO/RSI)?**	Los requisitos relativos a la formación y cualificación del perfil de Responsable de Seguridad de la Información (CISO/RSI) se encuentran recogidos en la DSA-SG-P01-GU02 Guía de evaluación de cargos responsables, disponible en la página web de AESA. https://www.seguridadaerea.gob.es/es/ambitos/aeronaves/guias-de-usuario---sistema-de-gestion
26	**¿Se conoce si la autoridad competente para la verificación del cumplimiento de la Directiva NIS2 aceptará la implementación de la Parte-IS como equivalente?**	AESA no es la autoridad competente para la verificación del cumplimiento de la Directiva NIS2. Por este motivo, no es posible confirmar si la implementación de la Parte-IS podría ser aceptada como equivalente en dicho ámbito.
27	**¿Puede una misma persona desempeñar simultáneamente los roles de Responsable de Seguridad de la Información Aeronáutica Civil (RSIAC) y Responsable del Control de Conformidad (RCC) para la Parte-IS?**	La figura del Responsable de Seguridad de la Información Aeronáutica Civil (RSIAC) no está contemplada en la Parte-IS de aeronavegabilidad continuada. En caso de que una organización cuente con dicha figura por estar sujeta a otras normativas o aprobaciones, la compatibilidad entre roles deberá evaluarse de forma individual, atendiendo a la estructura organizativa y a las funciones asignadas en cada aprobación. Si se desea plantear un caso concreto, se recomienda remitir la consulta detallada al buzón de SMGA para su valoración.
28	**En un holding con varias organizaciones y múltiples aprobaciones que comparten un**	No necesariamente. En aquellos casos en los que varias aprobaciones compartan un mismo RSI, podrá existir un único Director Responsable (DR) que asuma las funciones de coordinación sin necesidad de

	Responsable de Seguridad de la Información (RSI), ¿es obligatorio designar una Persona Responsable Común (CRP)?	designar un CRP. Alternativamente, el DR podrá delegar estas responsabilidades en una Persona Responsable Común (CRP), pudiendo ser esta o no el RSI común a todas las organizaciones, siempre que se garantice el cumplimiento de los requisitos establecidos para la Parte-IS.
29	**¿Deben reflejarse en el organigrama oficial de la organización las responsabilidades del CISO/RSIAC y su línea de reporte?**	Sí. Las responsabilidades asignadas al CISO/RSIAC, así como su posición dentro de la estructura organizativa y la línea de reporte correspondiente, deberán quedar reflejadas en el organigrama oficial de la organización y en la documentación aplicable del sistema de gestión.
30	**La guía no especifica qué apartados deben modificarse en el manual en caso de acogerse a una derogación. Indica que debe modificarse todo el manual y contiene referencias incorrectas. ¿Podrían aclararlo?**	AESA no puede especificar de manera universal qué apartados del manual deben modificarse, ya que cada organización puede haber incorporado referencias al SGSI en secciones, subapartados o procedimientos distintos, dependiendo de su estructura documental y de la casuística particular de cada aprobación. No obstante, la guía sí incluye una relación entre los puntos normativos y los apartados del manual, lo que permite identificar qué contenidos están vinculados con los requisitos del SGSI. A partir de dicha correspondencia, la organización podrá determinar qué apartados deben modificarse o eliminarse en caso de acogerse a una derogación, incorporando únicamente las referencias necesarias a los puntos aplicables.
31	**En el caso de solicitar una derogación y encontrarse la organización simultáneamente en proceso de otros cambios en el MOE, ¿deben remitirse únicamente los cambios relacionados con la Parte-IS?**	No. Tal como se indicó durante el webinar, la solicitud de derogación se gestiona como un cambio en la organización. Por tanto, no es necesario que la comunicación de cambios al MOE esté limitada exclusivamente a los aspectos relacionados con la Parte-IS; pueden incluirse otros cambios que la organización tenga en curso.
32	**La Parte-IS incluye en GM3 IS.I.OR.235 un listado de ejemplos de subcontratistas aplicables a esta normativa. ¿Deben dichas organizaciones considerarse dentro del alcance del SGSI, de modo que se reflejen en las auditorías internas o en los contratos? ¿Se entiende que un software, por sí mismo, no es un subcontratista, sino un producto o sistema crítico?**	De acuerdo con IS.I.OR.235(a), cuando una organización subcontrate tareas que estén dentro del ámbito de aplicación de la Parte-IS y que, de realizarse internamente, serían objeto de auditoría y control mediante los procedimientos establecidos en el SGSI, estas actividades subcontratadas permanecen igualmente dentro del alcance de la Parte-IS. En consecuencia, la organización sigue siendo responsable de garantizar el cumplimiento de los requisitos aplicables, verificando dicha conformidad conforme a los procedimientos recogidos en su manual del SGSI. En el caso del software, este no constituye un subcontratista por sí mismo. No obstante, dependiendo

		del tipo de servicio prestado por el proveedor del software y de la interacción o interfaz existente con la organización, dicho proveedor podría ser considerado como subcontratista a efectos de la Parte-IS.