Preguntas SLIDO Jornada PART-IS

Noviembre 2025

1. ¿Qué nivel de implementación del SGSI se exigirá tanto a la fecha de entrada en vigor de la Parte IS (22 de febrero de 2026)?
   Se exigirá que el SGSI esté presente y además que sea adecuado (al tamaño y complejidad de la organización). Posteriormente pasados 18 meses de la entrada en vigor, y en el marco de las auditorías de Sistema de Gestión del Plan de Vigilancia Continuada de cada operador, se verificará que este SGSI está operativo.

2. En el caso de varias compañías pertenecientes a un mismo grupo, algunas con más de una aprobación y donde todas comparten el RSI. ¿Es necesaria la figura de la Persona Responsable Común?
   Lo será en la medida en la que no existe un DR común a esas aprobaciones y sea necesario delegar en una sola figura la accountability y la provisión de recursos para cumplir con la Parte IS.

3. En el caso de varias compañías pertenecientes a un mismo grupo, algunas con más de una aprobación ¿se puede externalizar el RCC? ¿Actuaría éste como Focal Point y reportaría a cada uno de los RCC?
   Las actividades a realizar dentro de la Parte IS son susceptibles de ser subcontratadas, teniendo en cuenta que la responsabilidad última recae siempre en el operador. Dicho esto, al igual que ocurre con el SGS, la función de control de conformidad es única por sistema de gestión, por lo que a un SGSI le corresponde un solo RCC.

4. Cuando entre en vigor el Reglamento ¿habrá una auditoría específica de Part-IS o al auditar el SMS también se auditará el ISMS?
   Al solicitar la aprobación del MGSI o la modificación del MGS para incluir los aspectos de Seguridad de la Información, a realizar antes de febrero de 2026, se evaluará el MSGI y la evaluación de riesgos de seguridad de la información correspondiente y se evaluarán y aprobarán los cargos responsables. Se buscará que el SGSI esté presente y sea adecuado.
   Posteriormente a ello el SGSI será auditado con el SGS y dentro del marco del Plan de Vigilancia Continuada.

5. Si varias compañías del mismo grupo comparten el SGSI, ¿Se incluyen referencias en el SGSI al MSM o al revés?
   El SGSI en su definición de alcance deberá definir a qué organizaciones afecta, y por otro lado el Manual de Operaciones en su apartado A.3 o el MGS de cada organización deberá hacer referencia a ese SGSI y su versión vigente.

6. ¿Quién debería reportar a la autoridad (incidentes de seguridad de la información, gestión del cambio...) el RSI o el RS? ¿Y en el caso de que afecte a varias compañías de un mismo grupo es necesario reportarlas todas o con 1 reporte es suficiente? Es un único SGSI para todas.

En el caso de un único SGSI que afecta a varias organizaciones éste debe contar con su sistema de notificación tanto a nivel de reporte interno como de reporte externo, conforme a las provisiones de los puntos IS.I.OR.215 y IS.I.OR.230.
Dentro del SGSI es el RSI el encargado de gestionar este sistema de notificación y por tanto el responsable de su funcionamiento adecuado.
De la misma manera que se recomienda la integración del SGSI dentro del SGS, se recomienda esta acción para los sistemas de notificación, por lo que deberán claras en el MGSI las responsabilidades en cuanto a notificación tanto del RS como del RSI.

7. ¿Qué formación se requiere en Part-IS?
   La especificada para los cargos nominados y para el personal con responsabilidades de ciberseguridad detallado en el punto IS.I.OR.240

8. ¿Quién tiene que tener la formación?
   La especificada para los cargos nominados y para el personal con responsabilidades de ciberseguridad detallado en el punto IS.I.OR.240

9. ¿Es necesario incluir algo de Part-IS en la formación de concienciación en ciberseguridad para todos los empleados?
   Sí, el personal debe tener conciencia que los riesgos de seguridad de la información pueden derivar en riesgos de seguridad operacional y la importancia d esta transferencia.

10. ¿Qué formación en ciberseguridad deberían tener todo el staff responsable de la parte IS?
    La especificada para los cargos nominados y para el personal con responsabilidades de ciberseguridad detallado en el punto IS.I.OR.240

11. A nivel del alcance del ISMS, ¿debemos incluir todos los procedimientos relacionados con ciberseguridad aunque no tengan afectación en la seguridad operacional?
    El MSGI/SGSI debe dar alcance al tratamiento de riesgos de seguridad de la información con atención a los que pueden generar de manera potencial riesgos a la seguridad operacional. Por tanto, el desarrollo en profundidad de los procedimientos deberá atender a esa transferencia, pero debe desarrollarse y mantenerse la capacidad de evaluar en su conjunto las afecciones a la seguridad de la información para, desde esa visión global, focalizarse en la seguridad operacional.

12. En una compañía con varias aprobaciones ¿Cuál es la manera de entregar el MSGSI? ¿Se revisará de manera separada o se adjuntará con la presentación de otros Manuales?
    En compañía con aprobaciones AOC, CAMO y/o 145 la presentación del SGSI/MSGSI (integrado o independiente del SGS/MSG) se hará de la misma manera que en el caso del SGS/MSGS, presentándose a Operaciones (AOC). Si el SGSI/MGSI afecta a otras aprobaciones como por ejemplo una ATO, deberá seguirse el procedimiento establecido por el servicio correspondiente de AESA.

13. ¿Cuál es el canal habilitado por AESA para notificar sucesos de Seguridad de la Información ¿Será el mismo que para los sucesos de Seguridad Operacional?
    Deberán dirigirse al SNS de la misma manera que se hace con los de seguridad operacional. Está próxima la publicación de la modificación del Reglamento 376/2014 para inclusión de los casos de notificación obligatoria y de la tipología ECCAIRS.

14. ¿Es conveniente integrar el ISMS dentro del Sistema de Gestión del AOC?
    A juicio de AESA, aunque normativamente no es obligatorio, se cree muy conveniente y adecuado integrar en un solo sistema de gestión el actual SGS y el SGSI.

15. En una compañía con varias aprobaciones ¿Cuál es la manera de entregar el MSGSI? ¿Se revisará de manera separada o se adjuntará con la presentación de otros Manuales?
16. En compañía con aprobaciones AOC, CAMO y/o 145 la presentación del SGSI/MSGSI (integrado o independiente del SGS/MSG) se hará de la misma manera que en el caso del SGS/MSGS, presentándose a Operaciones (AOC). Si el SGSI/MGSI afecta a otras aprobaciones como por ejemplo una ATO, deberá seguirse el procedimiento establecido por el servicio correspondiente de AESA.
    Se evaluará de manera coordinada entre todas las partes interesadas dentro de AESA.

17. ¿CISO/RSI y PRC pueden ser la misma persona?
    Al igual que en el caso de la conjunción de los cargos de DR y RS en el SGS, la posibilidad de unir ambas funciones deberá ser previamente justificada y podrá tener sentido bajo unas condiciones determinadas, ligadas al tamaño y complejidad de la organización.

18. Se va a otorgar al operador una aprobación inicial al Part-IS, al manual, a los cargos? Los cambios sucesivos al manual y los procedimientos serán de aprobación o de notificación?
    No se otorga una aprobación específica al aprobarse el SGSI/MSGSI, al igual que no se hace al aprobarse (o modificarse) el SGS/MSGS. El operador deberá definir en su MSGSI un procedimiento que determine los cambios que requieren aprobación por parte de AESA y los que requieren notificación a AESA, siendo como mínimo de aprobación los mismos ítems que en el SGS/MSGS, es decir, líneas de responsabilidad (cargos responsables) y política y objetivos de seguridad.

19. ¿Qué formación en Safety debe recibir el RCP si este es un perfil de Seguridad de la Información?
    El RCP (CRP) ostenta un cargo que a nivel de formación en Sistemas de Gestión de Seguridad de la Información es similar al de DR, es decir, deberá cumplir los requisitos de formación especificados en “IS.I.OR.240 Requisitos de personal” relativos al DR.

20. ¿Podría utilizar la misma matriz de riesgo de mi SMS para Part-IS?
    Sí, puede usarse la misma matriz de riesgo y por tanto la misma metodología, adaptándola a las especificades de los riesgos de Seguridad de la Información.

21. ¿Si hay un incidente de Seguridad con impacto en Safety provocado por un evento de Seguridad de la Información, quién notifica? ¿Se notifica como incidente de seguridad de información y seguridad operacional? ¿Hay que duplicar las notificaciones?
    Deberá notificar la organización desde su SGSI, dirigiéndose al SNS de la misma manera que se hace con los de seguridad operacional. Está próxima la publicación de la modificación del Reglamento 376/2014 para inclusión de los casos de notificación obligatoria y de la tipología ECCAIRS, que tendrá en cuenta los sucesos de seguridad operacional que tienen un origen en seguridad de la información. No será necesario por tanto duplicar.

22. Podrían poner ejemplos de casos en los que habría que reportar un incidente según OR.230 (b)(2)? "... the organisation shall report it to the organisation responsible for the design of the system or constituent."

Por ejemplo, si en un sistema ACARS o similar se producen eventos de seguridad de la información como por ejemplo la perturbación de las comunicaciones afectando a su integridad o disponibilidad, deberá notificarse a la organización responsable del diseño del sistema para que evalúe la afección a su sistema y la posibilidad de introducir cambios en el diseño o uso del mismo.

23. Si aplico y recibo la derogación de AESA, ¿está mi organización exenta de cumplir con la Part-IS?
    Se estará exento de cumplir con todos los requisitos salvo los especificados en IS.I.OR.200 (e) y que se detallan y explican en el documento "DSA-SG-P01-GU05 Ed. 01 Guía solicitud derogación" en su apartado "3.5 Resumen de requisitos Reglamento 2023/203 (Parte IS)".
    Adicionalmente, la validez de la derogación se mantendrá en tanto en cuanto las condiciones por las que se otorgó se mantengan, extremo que deberá ser evaluado continuamente por la organización y por AESA en el marco del Plan de Vigilancia Continuada de la organización. Se pueden obtener más detalles a este respecto en el apartado "3.7 Validez de la aprobación y vigilancia continuada" de la mencionada Guía.

24. La evaluación de riesgos que se debe entregar para la aprobación ¿es la propia de la gestión del cambio (los riesgos que implica la entrada en vigor del nuevo reglamento) o es el análisis de todos los riesgos de seguridad de la información de la compañía?
    La evaluación de riesgos del SGSI debe comprender en primer lugar un acercamiento a la totalidad de los riesgos de seguridad de la información y una vez identificados aquellos que pueden generar un potencial impacto en la seguridad operacional, el análisis detallado de los mismos. No se limita a la simple Gestión del Cambio.

25. Una vez que ya se ha presentado el MSGI, Respecto a la documentación a presentar, ¿es necesario hacer modificaciones en el CAME o en el MO?
    Dependerá de la estructura elegida para implantar el SGSI (integrado, independiente y transversal para varias organizaciones, etc.). Como guía puede tenerse en cuenta que de la misma manera que el CAME o el MO refieran o incluyan el MSGS, en la misma línea deberá actuarse con el MSGSI. Cada caso será evaluado de manera particular durante el proceso de aprobación.

26. Es obligatorio seguir la estructura del ISMM que proponéis o bien es una guía?
    Por un lado, la estructura integrada o independiente del MSGSI con respecto al MSGS es libre, siendo la opción integrada la preferida por AESA.
    En cuanto a su estructura interna, la presentada en el apéndice al documento "DSA-SG-P01-GU01 Ed. 04 Guía del Manual del Sistema de Gestión" es una referencia y guía, que se complementa con el punto de la norma "GM1 IS.I.OR.250(a) Information security management manual (ISMM)".
    En todo caso deberá respetarse el contenido mínimo explicitado en IS.I.OR.250(a).

27. ¿Qué se debe presentar si se utiliza Pilar pata el análisis de riesgos? El análisis de riesgos es un fichero de Pilar. Se requiere ese fichero o un documento explicativa del proceso seguido y los resultados?
    Se requerirá un formato que pueda ser leído sin la herramienta PILAR o cualquier otra específica. Por ejemplo puede entregarse en formato Excel. La explicación del procesos seguido y sus resultados están comprendidos en la metodología elegida para la evaluación de riesgos de seguridad de la información, por lo que deberá ser parte del contenido del MSGSI.

28. No sería el ISMM lo que deberíamos presentar para valoración más que el SGSI? Al final el manual es la pieza que debería integrase dentro del MSG, en cambio el SGSI lo vemos mas bien como la arquitectura para su implementación.
    La documentación a entregar para la aprobación del SGSI se encuentra listada y detallada en las presentaciones de la Jornada y en el documento "DSA-SG-P01-GU01 Ed. 04 Guía del Manual del Sistema de Gestión".

29. ¿Quién debería ser el Responsable de Seguridad de la Información? ¿CISO, Cybersecurity Risk Manager, Cyber Incident Responder, NPs? ¿Debe reportar directamente al CRM?
    Deberá ser una persona nominada que cumpla con los requisitos detallados en el punto "IS.I.OR.240 Requisitos de Personal", para los que existe un documento de apoyo denominado "DSA-SG-P01-GU02 Ed. 04 Guía de evaluación de cargos responsables".
    CISO es un concepto proveniente de la certificación ISO 27001, el cual en la parte IS se recoge bajo la figura del RSI.

30. ¿Cómo se han planteado los requisitos mínimos que deben cumplir los proveedores (tanto tecnológicos como organizativos) para ser considerados válidos?
    Los requisitos tanto técnicos como organizativos de los proveedores de servicios o de las organizaciones a las que se proporcionan servicios (tanto los obligados al cumplimiento de la Parte IS como los que no) dependerán de la evaluación de los riesgos de seguridad de la información que se transfieren o se reciben a/desde estas organizaciones. Serán las barreras y medidas de mitigación que sea necesario implementar las que marcarán los requisitos mencionados.

31. ¿Cómo y de qué tipo se le puede dar formación específica al RSI?
    Puede encontrarse guía de la formación requerida para el RSI en el documento "DSA-SG-P01-GU02 Ed. 04 Guía de evaluación de cargos responsables".

32. ¿Se establecen requisitos de ciberseguridad a proveedores externos de los operadores aéreos (p.ej. fabricantes aviónica, comunicaciones, IFE, etc)?
    Sí, se requieren. Vendrán definidos por la evaluación de los riesgos de seguridad de la información que se transfieren o se reciben a/desde estas organizaciones. De ahí surgirán barreras y medidas de mitigación que será necesario implementar y que marcarán los requisitos de ciberseguridad mencionados.

33. En el caso de presentar una evaluación del riesgo que justifique que no estamos sometidos a un riesgo alto de IS, sería suficiente con modificar el SMS teniendo en cuenta la política de seguridad y notificación de sucesos de ciberseguridad?
    Una derogación al cumplimiento de la Parte IS sólo puede sustentarse en el punto normativo "IS.I.OR.200(e)", que requiere que tras evaluar los riesgos de seguridad de la información no exista potencial impacto de ninguno de ellos en la seguridad operacional.
    En tal caso podrá obtenerse una derogación al cumplimiento de la gran mayoría de requisitos de la Parte IS salvo los mencionados en el punto "IS.I.OR.200(e)".
    En cualquier otro caso deberá implementarse un SGSI y solicitarse la aprobación del mismo.
    Para más detalle pueden consultarse los documentos "DSA-SG-P01-GU01 Ed. 04 Guía del Manual del Sistema de Gestión" y "DSA-SG-P01-GU05 Ed. 01 Guía solicitud derogación".

34. En el caso de One BG (AOC, CAMO, 145), ¿ a que unidad de AESA se ha de presentar el cambio?

En compañía con aprobaciones AOC, CAMO y/o 145 la presentación del SGSI/MSGSI (integrado o independiente del SGS/MSG) se hará de la misma manera que en el caso del SGS/MSGS, presentándose a Operaciones (AOC). Si el SGSI/MGSI afecta a otras aprobaciones como por ejemplo una ATO, deberá seguirse el procedimiento establecido por el servicio correspondiente de AESA.
Se evaluará de manera coordinada entre todas las partes interesadas dentro de AESA.

35. En nuestra organización (operador Handling), es tema IT, sistemas etc es subcontratado, existe un responsable de ciberseguridad/ RSI externo nombrado. De cara al SGSI, es necesario tener un figura interna como RSI ?
Sí, debe nombrarse un responsable interno en la organización.

36. Se ha comentado que los responsables son evaluados y aprobados por parte de AESA. ¿Esto se va a realizar de forma documental o serán entrevistas personales a los responsables propuestos?
Se procederá de la misma manera que con el resto de cargos responsables de la organización. Puede consultarse el documento "DSA-SG-P01-GU02 Ed. 04 Guía de evaluación de cargos responsables".

37. Para un operador que tiene varias aprobaciones AOC, CAMO, 145 y la parte IS externa con un único manual, se auditará esta parte IS en cada auditoría de cada aprobación?
Se procederá a auditar conforme al PVC del SGS de cada organización.

38. ¿Cómo se integrará la Parte IS con otras normativas coincidentes como SA-16, ENS, NIS2, etc?
Las organizaciones que deban cumplir en concreto con NIS2 y AVSEC podrán encontrar equivalencias y sinergias entre estas reglamentaciones y la Parte IS. En todo caso el cumplimiento de requisitos Parte IS no podrá ser automáticamente validado mediante el cumplimientos de éstas, siendo siempre necesario un análisis de equivalencia de sus requisitos con los de la Parte IS.

39. ¿Pueden explicar con más detalle cómo se aprobará el manual parte IS en aquellas organizaciones que tenemos múltiples aprobaciones (CAT, SPO, CAMO, 145, ATO, COE) y que optamos por un sistema de IS común para todas?
En compañía con aprobaciones AOC, CAMO y/o 145 la presentación del SGSI/MSGSI (integrado o independiente del SGS/MSG) se hará de la misma manera que en el caso del SGS/MSGS, presentándose a Operaciones (AOC). Si el SGSI/MGSI afecta a otras aprobaciones como por ejemplo una ATO, deberá seguirse el procedimiento establecido por el servicio correspondiente de AESA.
Se evaluará de manera coordinada entre todas las partes interesadas dentro de AESA.

40. Buenos días, ¿Se prevé una extensión en la implementación de la norma?
No, no se prevé.

41. En el caso de un grupo empresarial, ¿es necesario un MSGI para cada organización? ¿O es suficiente con uno para el grupo dejando clara las responsabilidades?
En grupos empresariales con varias aprobaciones la presentación del SGSI/MSGSI bien se presente integrado bien se presente independiente se centralizará de la misma manera que se hace con el SGS/MSGS, presentándose a Operaciones (AOC) y notificando a título informativo a los Principales del resto de aprobaciones. Internamente AESA coordinará la evaluación de la solicitud.

42. ¿ Cómo presentamos el F-001 para aprobación del MSGSI sino recoge todavía los nuevos cargos responsables?
    Mientras no se encuentre disponible la versión actualizada del F01, será suficiente con presentar el nuevo formato "DSA-SG-P01-F12 Ed. 01 Lista chequeo requisitos ISMS operadores".

43. Respecto al proceso de aprobación, ¿dónde podemos encontrar la lista de comprobación de cumplimiento que se ha mostrado en la presentación?
    En el siguiente enlace:
    https://www.seguridadaerea.gob.es/ambitos/operaciones-aereas/transporte-aereo-comercial-cat/normativa-y-material-guia

44. ¿Dónde pueden descargarse las herramientas de identificación de activos y de compliance que se han comentado durante la intervención de Binter?
    Binter usa la metodología Magerit, cuya herramienta es la aplicación PILAR. Puede encontrarse más información en los siguientes enlaces:

    https://pilar.ccn-cert.cni.es/metodologia/metodologia-pilar
    https://pilar.ccn-cert.cni.es/pilar/que-es-pilar

    Adicionalmente, puede encontrarse un listado de amenazas en el Apéndice 1 del Anexo II del Reglamento 2023/203.

45. ¿La aprobación del SGSI se hará a través del F001?
    Cuando esté disponible la nueva versión que incluya Parte IS, así será. Mientras tanto debe hacerse uso del formato "DSA-SG-P01-F12 Ed. 01 Lista chequeo requisitos ISMS operadores".

46. ¿Existe un banco de Amenazas para hacer la evaluación de riesgos, o un modelo-guía de la misma?
    Puede encontrarse un listado de amenazas en el Apéndice 1 del Anexo II del Reglamento 2023/203.

47. ¿Hay un plazo límite determinado (o, en caso negativo, cuál puede ser el plazo máximo razonable) para la presentación de solicitudes de derogación parcial?
    Se espera de los operadores que como mínimo con una antelación de dos meses a la entrada en vigor de la parte IS se haya registrado la solicitud de derogación. En caso negativo, no se puede asegurar que pueda tramitar en tiempo y forma la solicitud.
    Llegado el día de entrada en vigor, a las organizaciones que no se hayan derogado o les haya sido aprobado su SGSI se les levantará una discrepancia de nivel 2 al respecto otorgando el plazo habitual para su subsanación.

48. ¿Qué condicionas de derogación y de no aplicabilidad existen para organizaciones CAMO y ATO? (Aeronaves y organizaciones no complejas?
    Desde Operaciones no podemos dar respuesta a estas cuestiones, por lo que se ruega se contacte directamente con el Buzón de Aeronavegabilidad Continuada y/o con el de Organizaciones ATO.

49. ¿Qué ocurre si la actuación del PVC correspondiente al SGS tiene lugar antes del 22 de febrero de 2026, se revisará la Parte IS o se dejará para la siguiente actuación? Y en caso de revisarse, ¿se mirará si está presente y es adecuado, o también si es operacional?

Antes del 22 de febrero en ninguna actuación de PVC se exigirá el cumplimiento de la Parte IS. Sólo se hará a partir del 22 de febrero y conforme al PVC establecido para cada organización. Tanto durante la evaluación de la aprobación como durante la primera actuación de PVC en la que se evalúe el SGSI sólo será necesario que esté presente y sea adecuado.

50. La normativa pide la comprobación de antecedentes, ¿valdría entregar por los empleados un justificante de consulta de ausencia o debe ser un certificado oficial al uso?

    La norma no exige un formato determinado de comprobación de los antecedentes del trabajador. Sí exige que estos sean comprobados, dependiendo el alcance de esta comprobación aspectos tales como las características del puesto de trabajo o el respeto al resto de la legalidad vigente.

    En todo caso, el alcance de esta comprobación deberá ser especificado en el MSGSI.