



MINISTERIO
DE TRANSPORTES
Y MOVILIDAD SOSTENIBLE



Evolución implantación del Sistema de Gestión Temas Varios AESA - Inspecciones

Fco. Javier Carvajal Bricio
Jefe de la División de Aeronavegabilidad Inicial
Madrid, 15-06-2025

1. Resumen Parte IS
2. Fase Operativa de los Sistemas de Gestión
3. Comentarios “Procesos de Supervisión”





Parte IS

- **Definir Alcance**
- **Evaluar Impacto de la Parte IS → Solicitud**
 - **Derogación (implementación X%)**
 - **Implementación (Implementación 100%)**
- **Acciones:**
 - **Procedimientos.**
 - **Indicadores**
 - **Personal**
 - **Procesos**
 - **Sistemas**
 - **Contratos de personal**
 - **Suministradores (subcontratistas) → Contratos**
- **Aprobación del Cambio / derogación**
- **Implementación / supervisión**

16 / octubre / 2025

Supervisión PVC





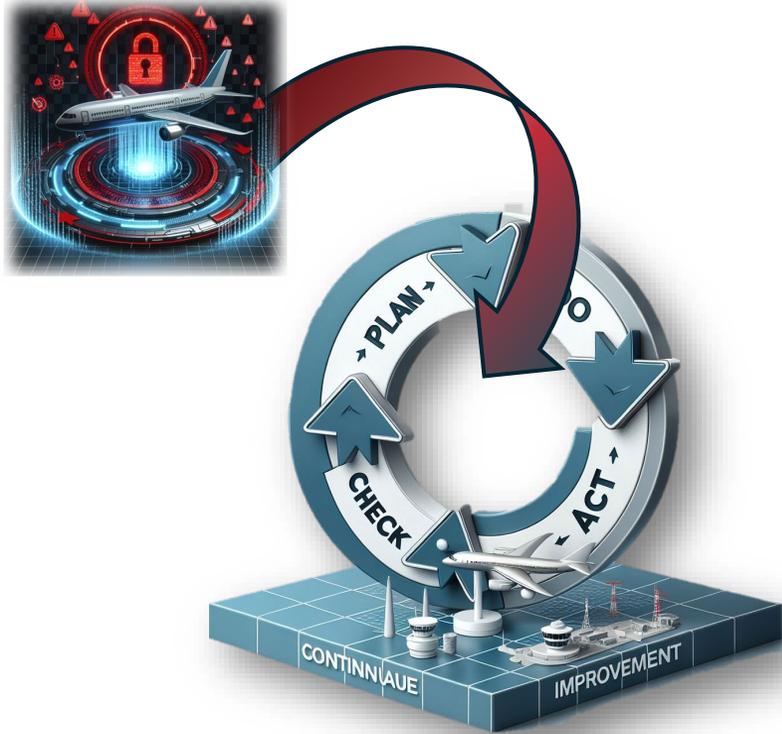
Contenido Parte IS

| | |
|-------------|--|
| IS.D.OR.100 | Ámbito de aplicación |
| IS.D.OR.200 | Sistema de gestión de la seguridad de la información |
| IS.D.OR.205 | Evaluación de los riesgos relacionados con la seguridad de la información |
| IS.D.OR.210 | Tratamiento de los riesgos relacionados con la seguridad de la información |
| IS.D.OR.215 | Sistema interno de notificación en materia de seguridad de la información |
| IS.D.OR.220 | Incidentes con la seguridad de la información: detección respuesta y recuperación |
| IS.D.OR.225 | Respuesta a las incidencias notificadas por la autoridad competente |
| IS.D.OR.230 | Sistema externo de notificación en materia de seguridad de la información |
| IS.D.OR.235 | Contratación de actividades de gestión de la seguridad de la información |
| IS.D.OR.240 | Requisitos relativos al personal |
| IS.D.OR.245 | Conservación de registros |
| IS.D.OR.250 | Manual de gestión de la seguridad de la información (MGSI) |
| IS.D.OR.255 | Cambios en el sistema de gestión de la seguridad de la información |
| IS.D.OR.260 | Mejora continua |

| | |
|--------------|---|
| 21.A.131 | Ámbito de aplicación |
| 21.A.139 | Sistema de gestión de la producción |
| 21.A.139 c.3 | Sistema de gestión de la producción |
| 21.A.139 c.3 | Sistema de gestión de la producción |
| 21.A.3A | Sistema de notificación |
| 21.A.158 | Incidencias y observaciones |
| 21.A.3A | Sistema de notificación |
| 21.A.3A | Sistema de notificación |
| 21.A.139 d) | Sistema de gestión de la producción |
| 21.A.145 | Recursos |
| 21.A.5 | Conservación de registros |
| 21.A.143 | Memoria. Parte 3 |
| 21.A.147 | Cambios en el sistema de gestión de la producción |
| | |



PELIGRO



- NO ES LO MISMO -



- *Cambio de mentalidad y de cultura*
- *Difusión / Formación*
- *Recursos → Responsables*
- *Recursos → Personal*
- *Actualización de contratos*





FAQ EASA: ¿Es necesario proteger la información sólo de las amenazas digitales o también de las no digitales?

El uso del **término «seguridad de la información»** en la Parte-IS, en contraposición a «ciberseguridad», **es deliberado y significativo**. Se ha elegido para abarcar una gama más amplia de riesgos asociados a los sistemas de información.

«ciberseguridad», → Se centra en la protección de los datos frente a las amenazas digitales

«seguridad de la información» → se extiende más allá e incluye las amenazas analógicas.

Se reconoce que las vulnerabilidades y amenazas a los sistemas de información pueden surgir tanto en formato digital como físico, lo que requiere un mayor alcance de medidas y consideraciones de protección.

PELIGRO - ¿Exterior, interior?

IS.D.OR.240 Requisitos relativos al personal

i) La organización **velará por que se establezca adecuadamente la identidad y la fiabilidad del personal** que tenga acceso a los sistemas de información y a los datos sujetos a los requisitos del presente Reglamento.

AMC1 IS.D.OR.240(i) Personnel requirements

Para el personal con acceso a los sistemas de información y datos sujetos a los requisitos de la Parte IS, **la identidad debe determinarse mediante pruebas documentales**. Para establecer la confiabilidad de dicho personal, la organización debe contar con un proceso documentado y criterios adecuados que garanticen que se puede confiar en las personas para el desempeño de sus funciones.

GM1 IS.D.OR.240(i) Requisitos de personal

- (a) La fiabilidad podrá determinarse, por ejemplo, mediante una verificación de antecedentes previa al empleo y podrá incluir la verificación de:
- (i) formación, empleos anteriores y cualquier carencia en los años anteriores;
 - (ii) **ausencia de antecedentes penales;**
 - (iii) cualquier otra información o inteligencia pertinente que se considere relevante para la idoneidad de una persona para el puesto previsto;





Part-IS Implementation Workshop 2024

Part-IS Implementation Workshop 2025 (25-26 junio)

Part-IS Oversight Approach Guidelines

Procedimiento y guías de AESA





MANUAL → ¿Qué me permite la norma?

- POE (Incluido el SG y el SGI)



- **POE + MSG + MGS**

- POE + MSG/MSGI





Metodología seguida por EASA para la implementación de los SG y SGI

Enfoque P.S.O.E.:

- Presente: Los requisitos normativos están claramente visibles, documentados y existen evidencias de la incorporación dentro de la documentación del SMS de la organización.
- Adecuado: La documentación es adecuada en función del tamaño, naturaleza, complejidad y el riesgo inherente en la actividad de la Organización.
- Operativo: Hay evidencia de que el SG y el SGI está en uso y se está produciendo un resultado.
- Efectivo: Hay evidencia de que el SG y el SGI está logrando efectivamente el resultado deseado.



No es un requisito normativo





*Metodología seguida por EASA para la implementación de los **SG** y **SGI***

Presente

Adecuado

Operativo

Efectivo



Indicadores

Implementación de medidas de mitigación, acciones, etc..

Gestión del Cambio

Difusión de la política

Política de notificación

Reportes internos / externos (registros, implementación..)

Formación SG



Metodología seguida por EASA para la implementación de los SG y SGI



CLAVES en esta FASE (SG Operativo)

Compromiso de la dirección.

No pueden existir “*finding*” sobre los conceptos básicos ya aprobados (Present & suitable)

Las acciones internas y medidas mitigadoras se aplican y se revisan.

Implementación de cambios tras procesos de evaluación / actuación / mitigación

Personal de la organización con conocimiento/información (política, reporte, etc...)

Evolución de indicadores (registros, análisis, cambios, etc...)

Reportes internos / externos (registros, implementación..)

Supervisión y revisión de la efectividad del sistema de gestión (interno)



Supervisión y revisión de la efectividad del sistema de gestión



Mejora continua del SG



¿Cómo conseguirla?

- Valoraciones de cómo funciona la gestión de seguridad.
- Identificación y análisis de posibles retos asociados con el funcionamiento de la gestión de seguridad.
- Implementación de cambios para la mejora de la gestión de seguridad.
- Seguimiento y revisión de los efectos de cualquier cambio.

¿,Cómo podría mejorarse su rendimiento?

- Procedimientos de aprendizaje.
- Mejoras en las revisiones de seguridad, estudios de seguridad y auditorías.
- Mejoras en el sistema de reporte y herramientas de análisis.
- Mejoras en los procesos de identificación y evaluación de peligros y de concienciación en materia de riesgos en la organización.
- Mejoras en las relaciones con los subcontratistas, proveedores y clientes en lo relativo a la seguridad.
- Mejoras en los procesos de comunicación, incluyendo feedback del personal



COMENTARIOS PROCESOS DE SUPERVISIÓN

1. Adaptación de los ciclos de PVC (Importancia de los subcontratistas)
2. Responsabilidad sobre la firma de Form 1 / Certificado de conformidad
3. Alcance de la Organización → Dato de Diseño
4. Form 1 → Dato de diseño
5. Gestión de Manuales (POE), contenido según 21.A.143 →
6. Gestión de discrepancias :
 1. Cumplimentación de PAC,
 2. Cumplimiento de plazos,
 3. Tiempos acordes al finding, etc...



Gracias por su atención

www.seguridadaaerea.gob.es