MINISTERIO
DE TRANSPORTES
Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL
DE SEGURIDAD AÉREA

# Implementación Part-IS desde la perspectiva de la Autoridad

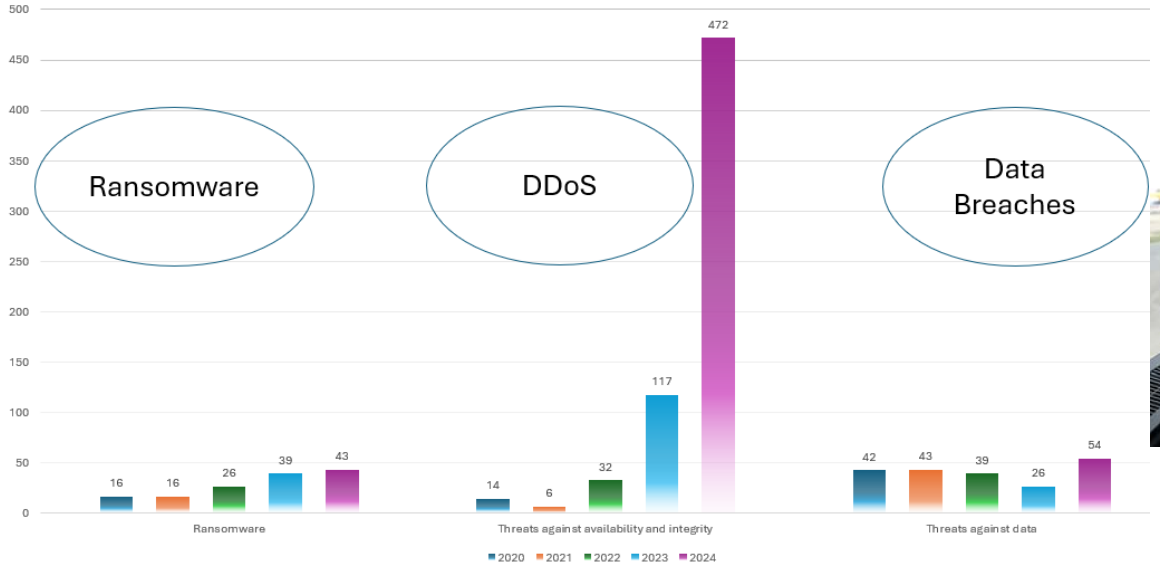
Francisco VALERO PADRÓN
Servicio de Helicópteros y Trabajos Aéreos
Madrid, 13-noviembre-2025

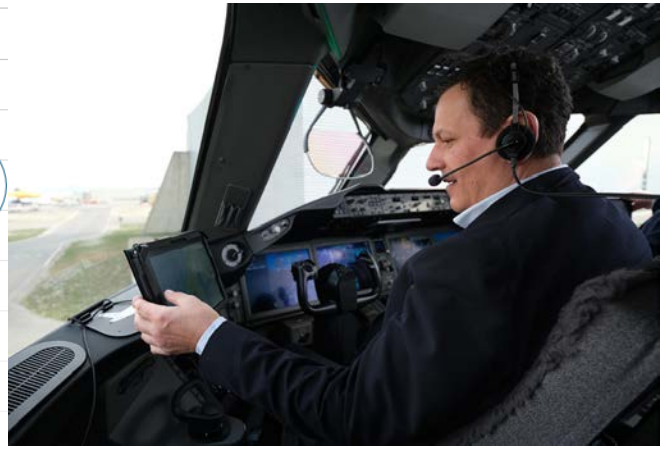
# Índice

1. Introducción a la Parte IS
2. La relación entre SGS y SGSI
3. Los cargos responsables en el SGSI
4. La evaluación de riesgos en el SGSI
5. Parte IS y otras organizaciones
6. Gestión de incidencias
7. Notificación interna y externa
8. Proceso de aprobación del SGSI
9. Conclusiones

# 1. Introducción a la Parte IS

## ¿ QUÉ NIVELES DE INFORMACIÓN CRECIENTE SE MANEJAN EN LA ACTIVIDAD AÉREA?



Los sistemas usados en la aviación intercambian INFORMACIÓN que representa barreras clave de SEGURIDAD y permite la adecuada OPERATIVIDAD. Debe ser

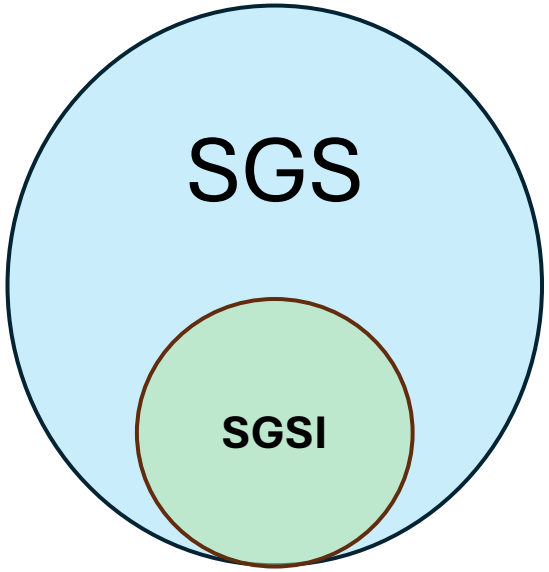
Los SISTEMAS DE INFORMACIÓN deben ser protegidos de accesos no autorizados, uso indebido, distribución no autorizada, modificación no autorizada y de la propia destrucción física.

*Confidencialidad *Integridad *Disponibilidad

# 2. La relación entre SGS y SGSI

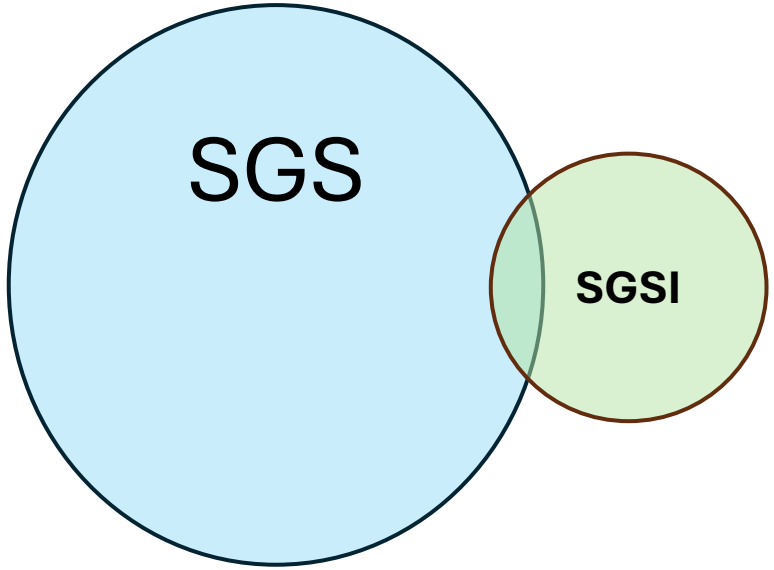
# 2. La relación entre SGS y SGSI

## SGSI integrado




- Aprovechar las políticas y procedimientos existentes
- Coherencia con el enfoque de gestión general de la organización.
- Sinergias en los procesos de gestión de riesgos existentes
- Reutilizar los controles existentes y el sistema de notificación
- Mejor coordinación interna y foco en la Seguridad Operacional
- Aplicable a la gran mayoría de operadores

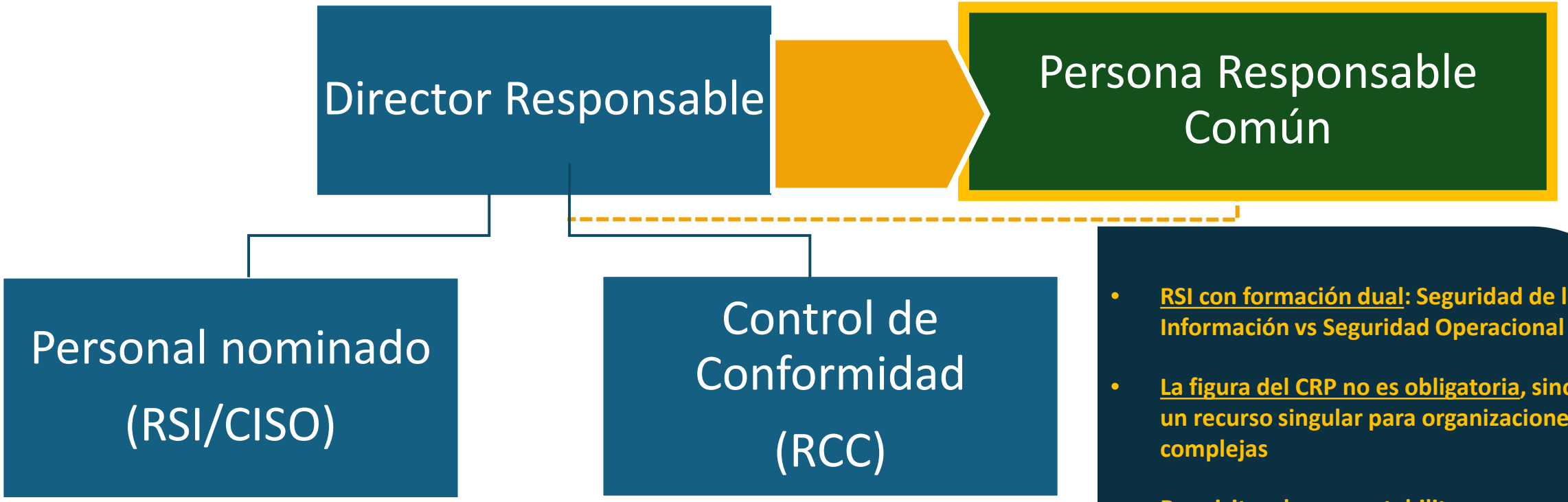
## SGSI independiente




- Duplicación de estructuras con la necesaria coordinación
- Idóneo en casos singulares (e.g. grupos empresariales diversos con organizaciones relacionadas)
- Mayor posibilidad de asignación de recursos

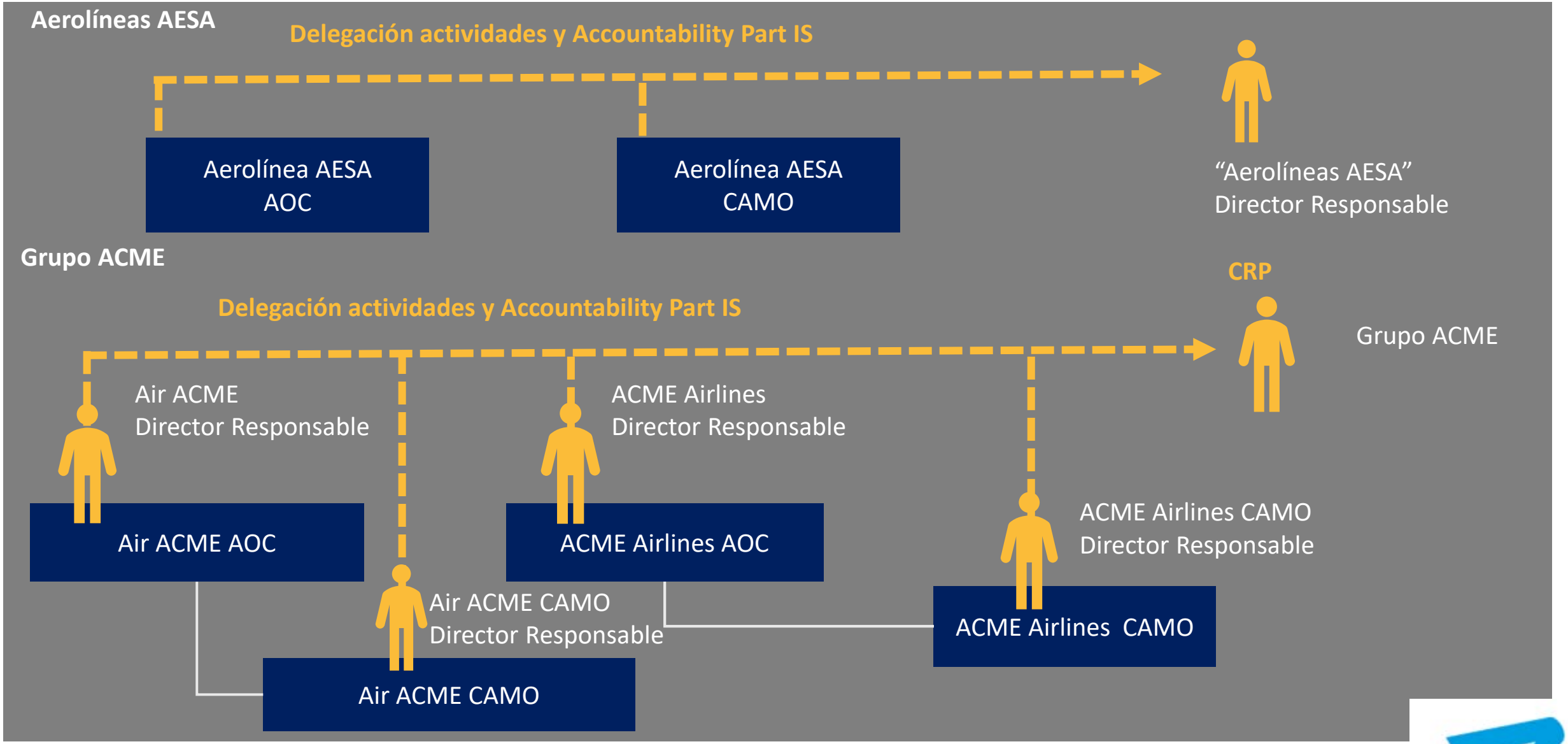
# 3. Los cargos responsables en el SGSI

# 3. Los cargos responsables en el SGSI

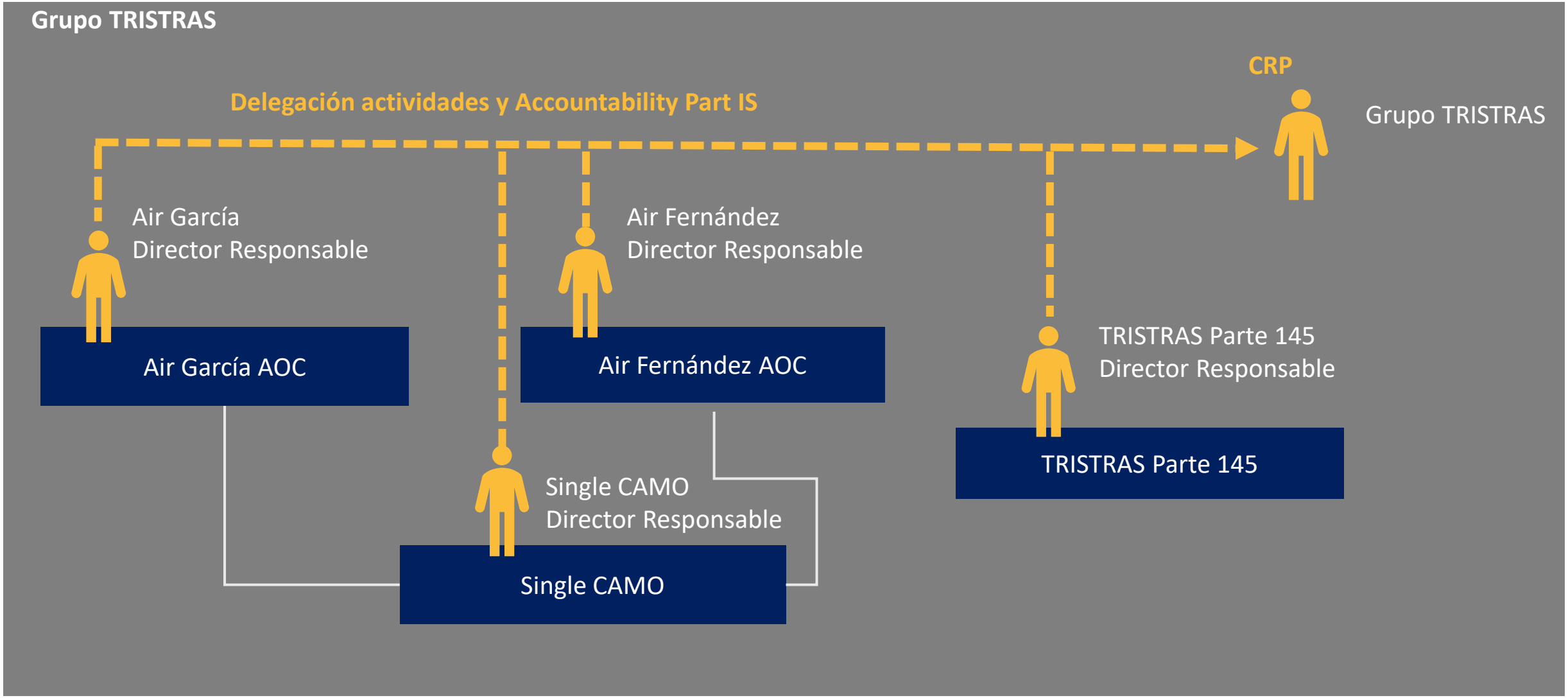



- **RSI con formación dual: Seguridad de la Información vs Seguridad Operacional**
- **La figura del CRP no es obligatoria, sino un recurso singular para organizaciones complejas**
- **Requisitos de accountability**
- **Funciones ejecutivas**

# 3. Los cargos responsables en el SGSI

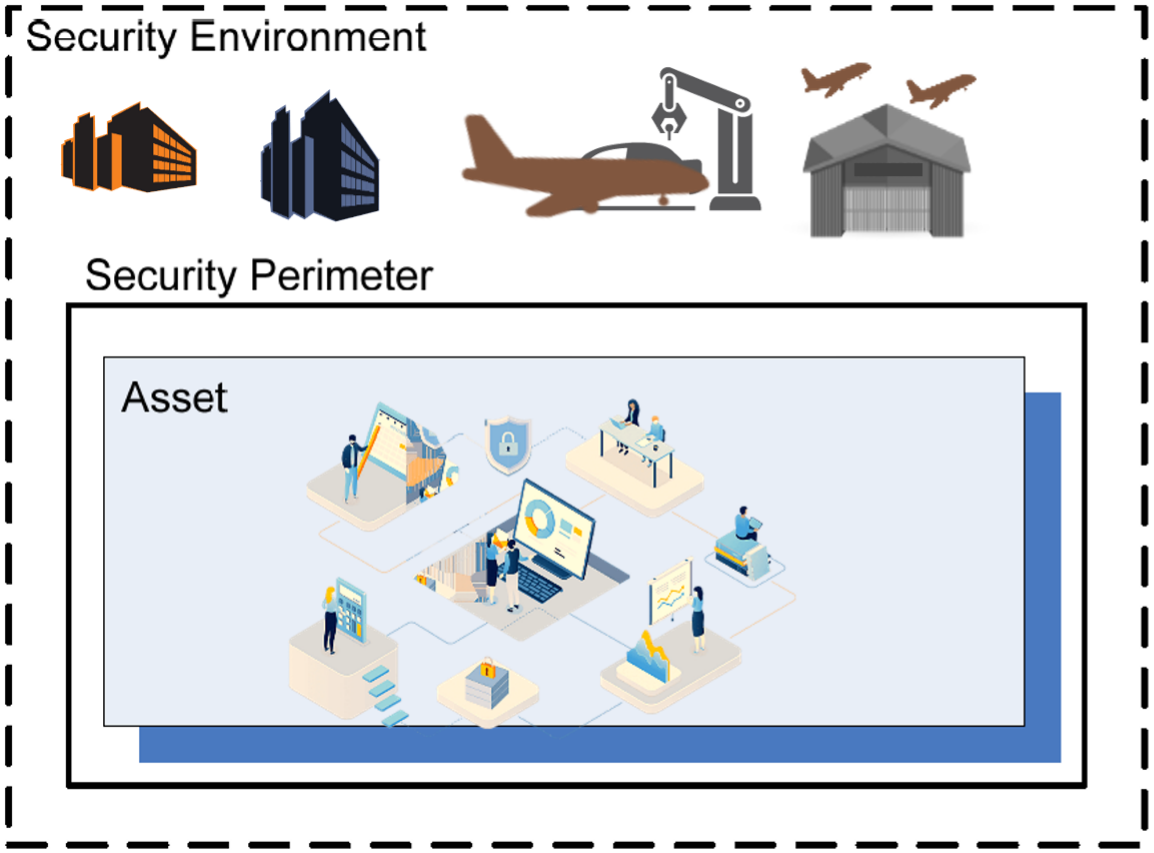


# 3. Los cargos responsables en el SGSI



# 4. La evaluación de riesgos en el SGSI

## DEFINICIÓN DE INTERFACES Y ACTIVOS DE LA ORGANIZACIÓN



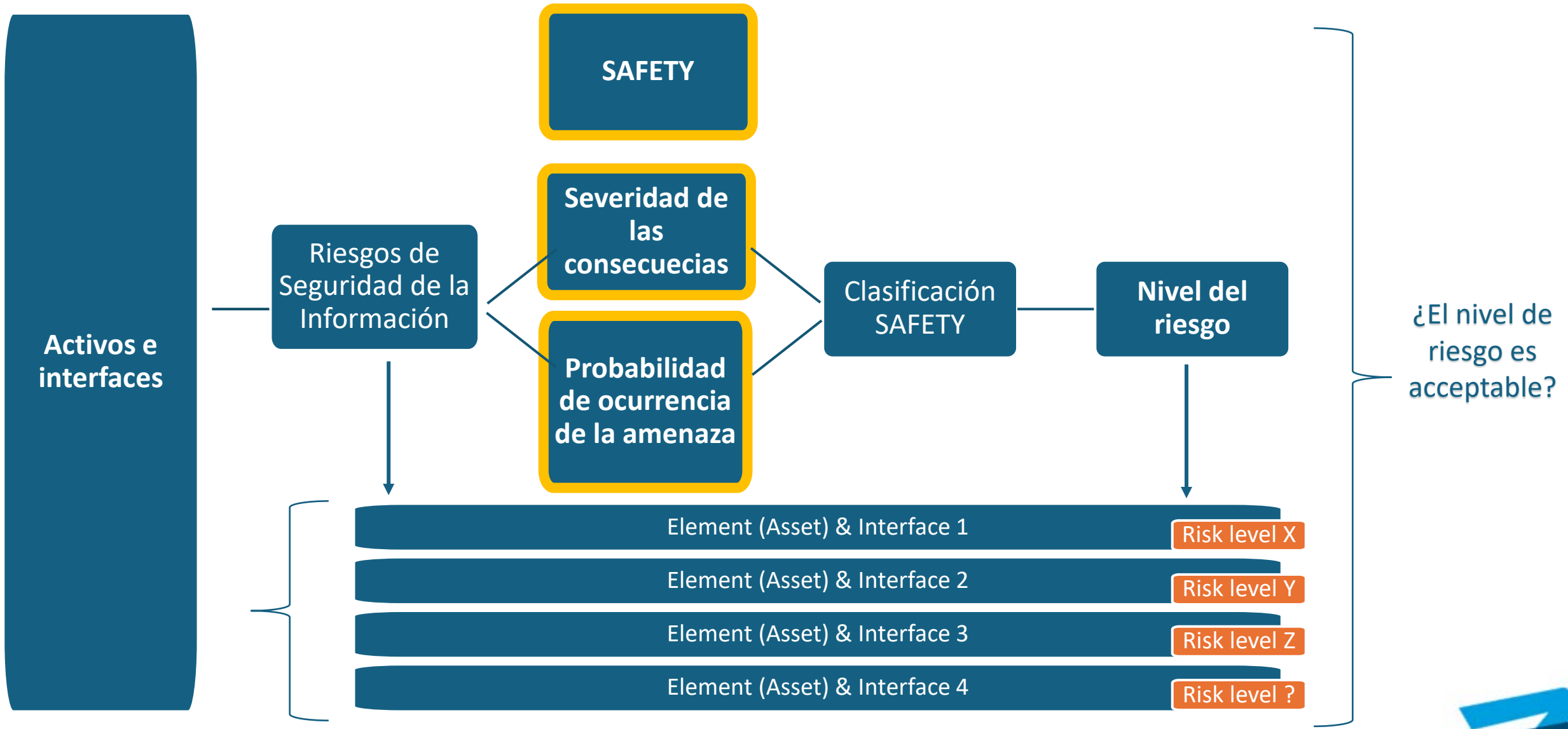

| Elements (Assets) |
| --- |
| Organisation's activities, facilities and resources |
| Services the organisation operates, provides receives or maintains |
| Equipment, systems, data and information |

| Interfaces with other organisations |
| --- |
| Interactions between elements |

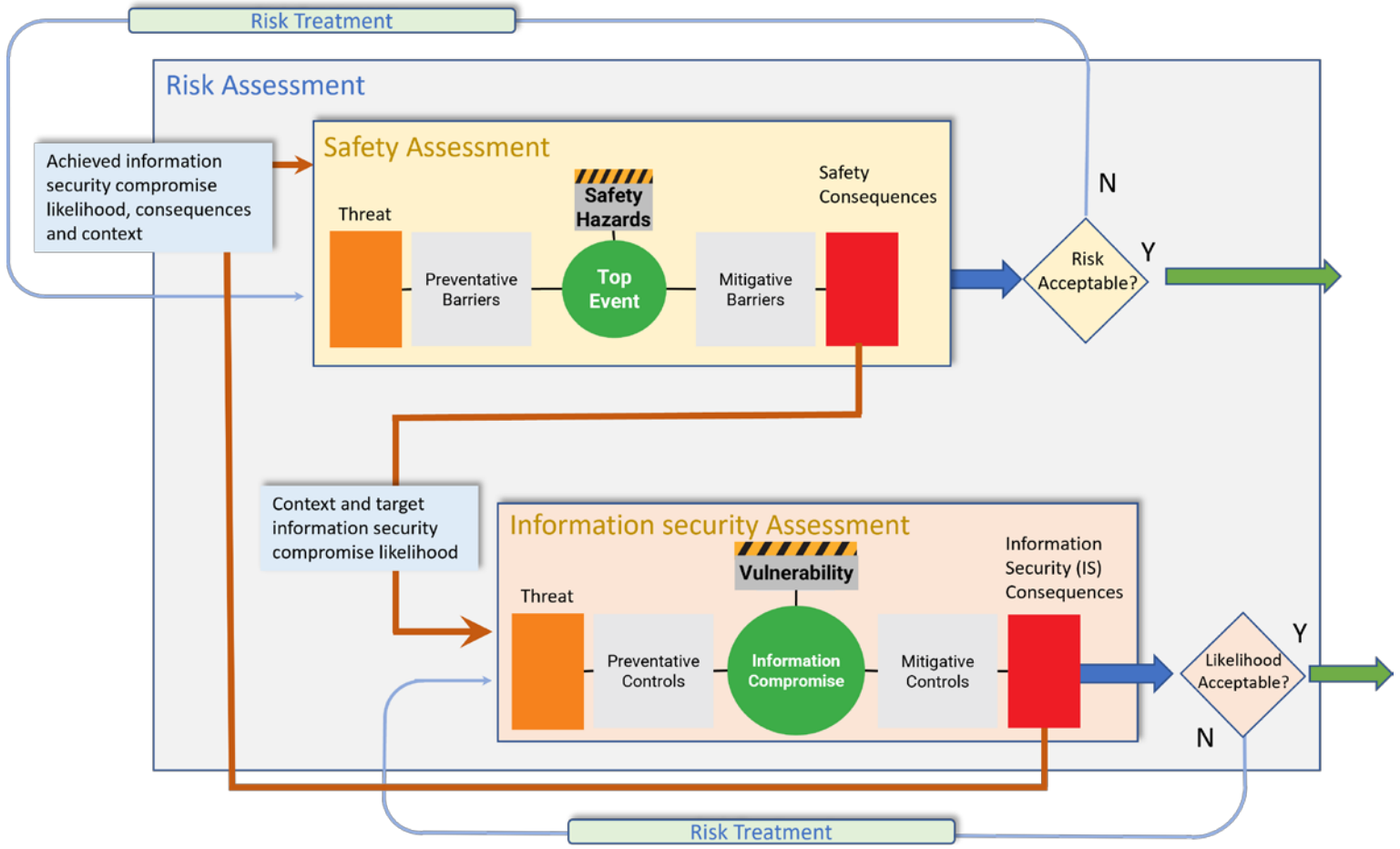
Safety

Methodology adopted to perform the scope analysis

# 4. La evaluación de riesgos en el SGSI

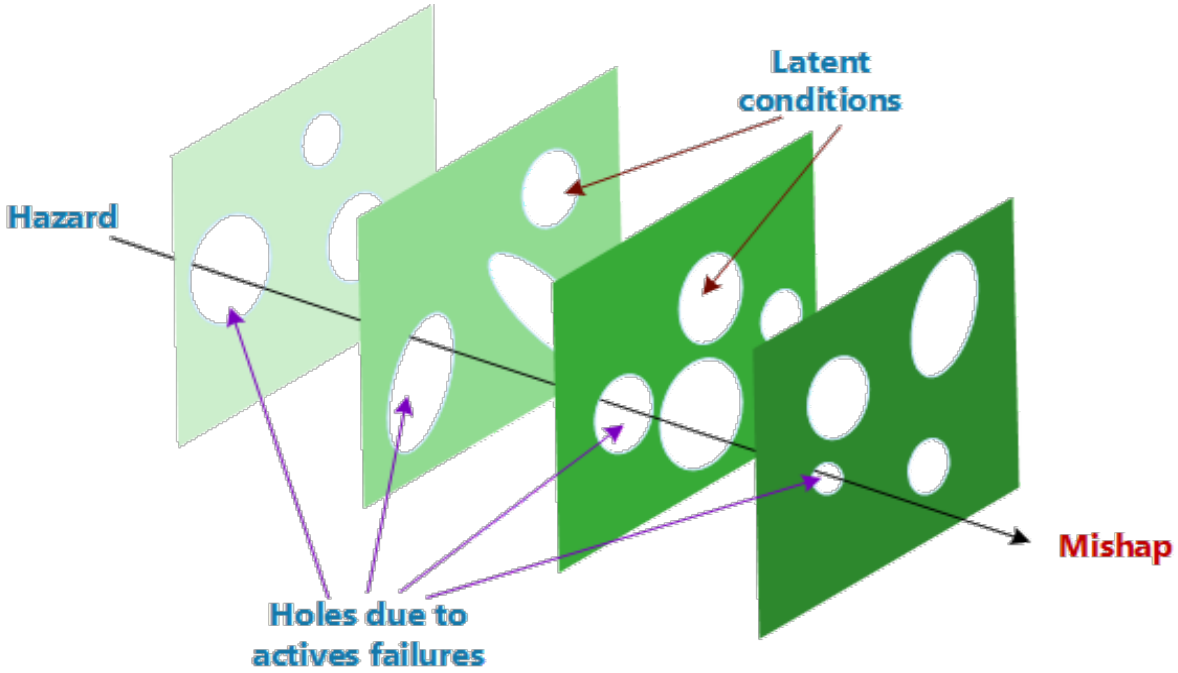


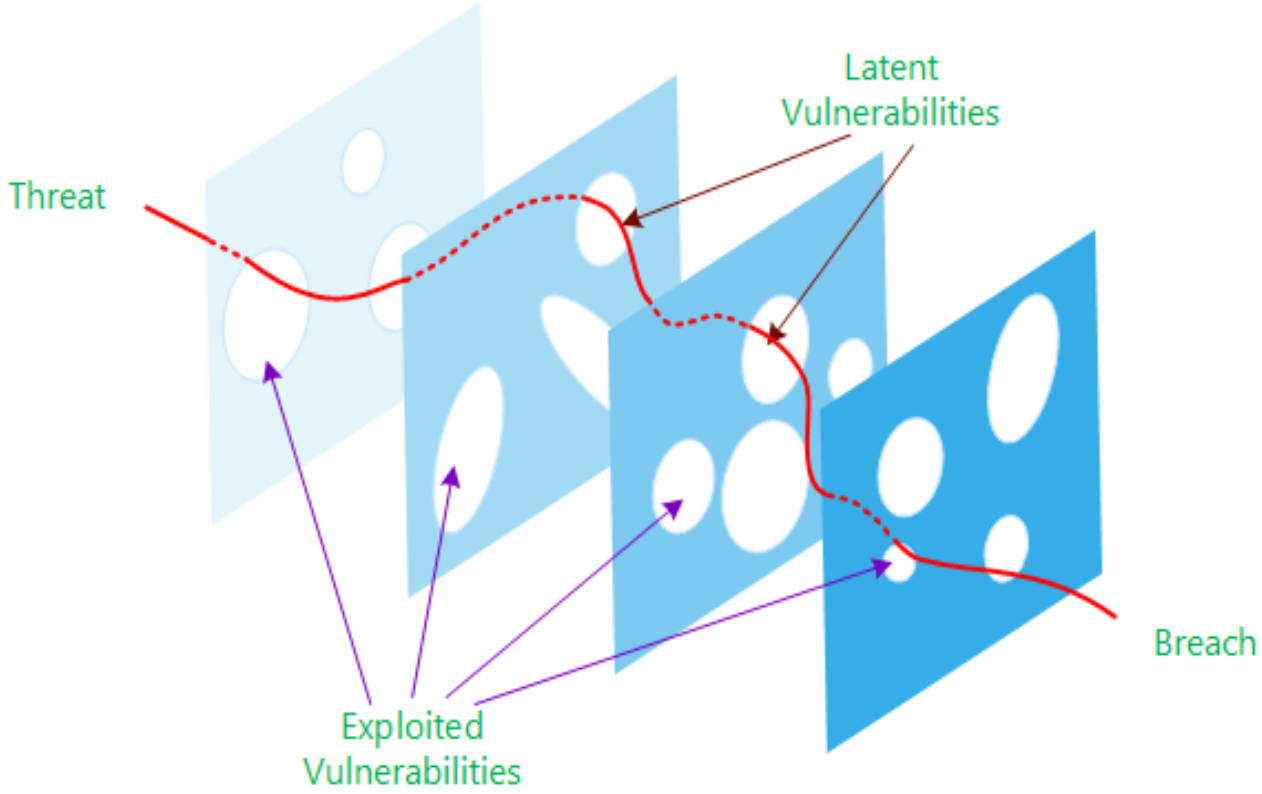
## ¿Cómo interactúa la evaluación del riesgo de seguridad de la información vs seguridad operacional?




**La Parte IS no exige el uso de ningún marco específico de evaluación de riesgos**

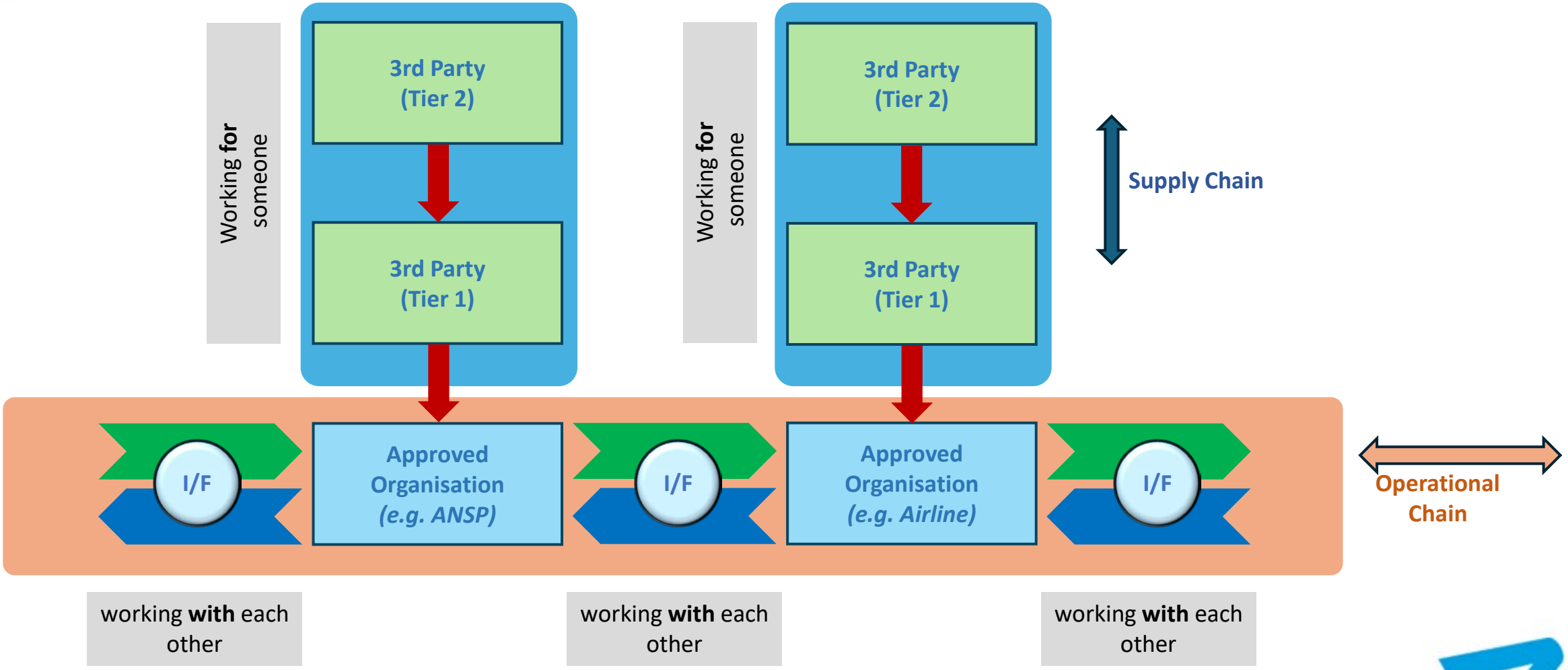
## SAFETY vs SECURITY



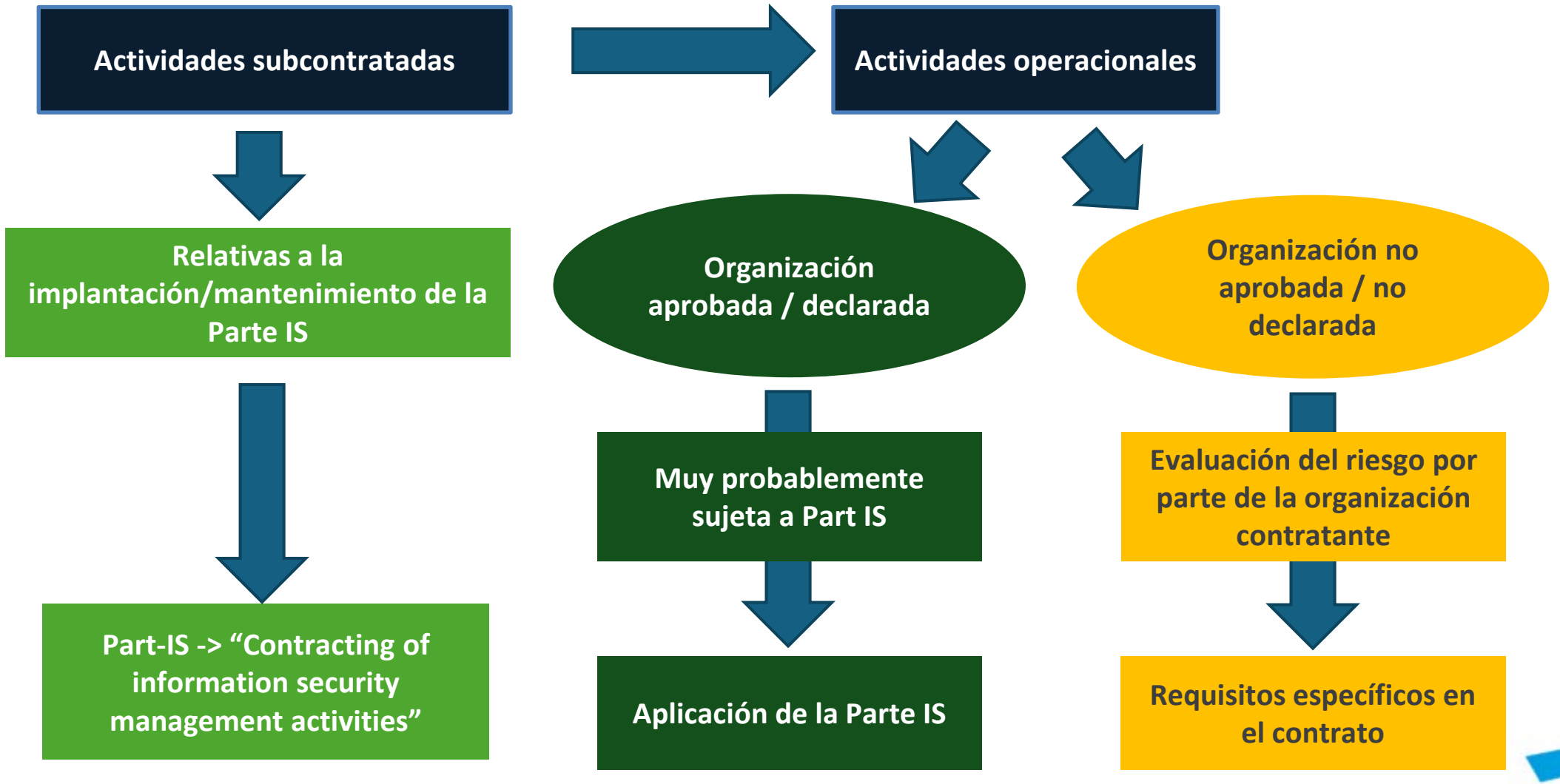



# 5. Parte IS y otras organizaciones

## ¿Qué significa "cadena funcional"?



# 5. Parte IS y otras organizaciones



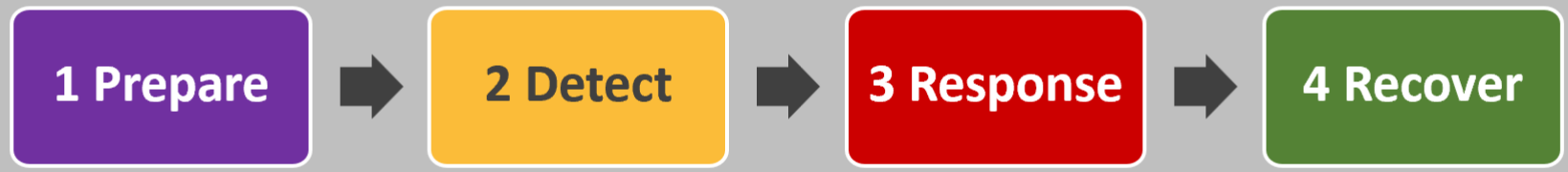
# 6. Gestión de incidencias

# 6. Gestión de incidencias

## Gestión de incidencias: detectar, responder, recuperarse

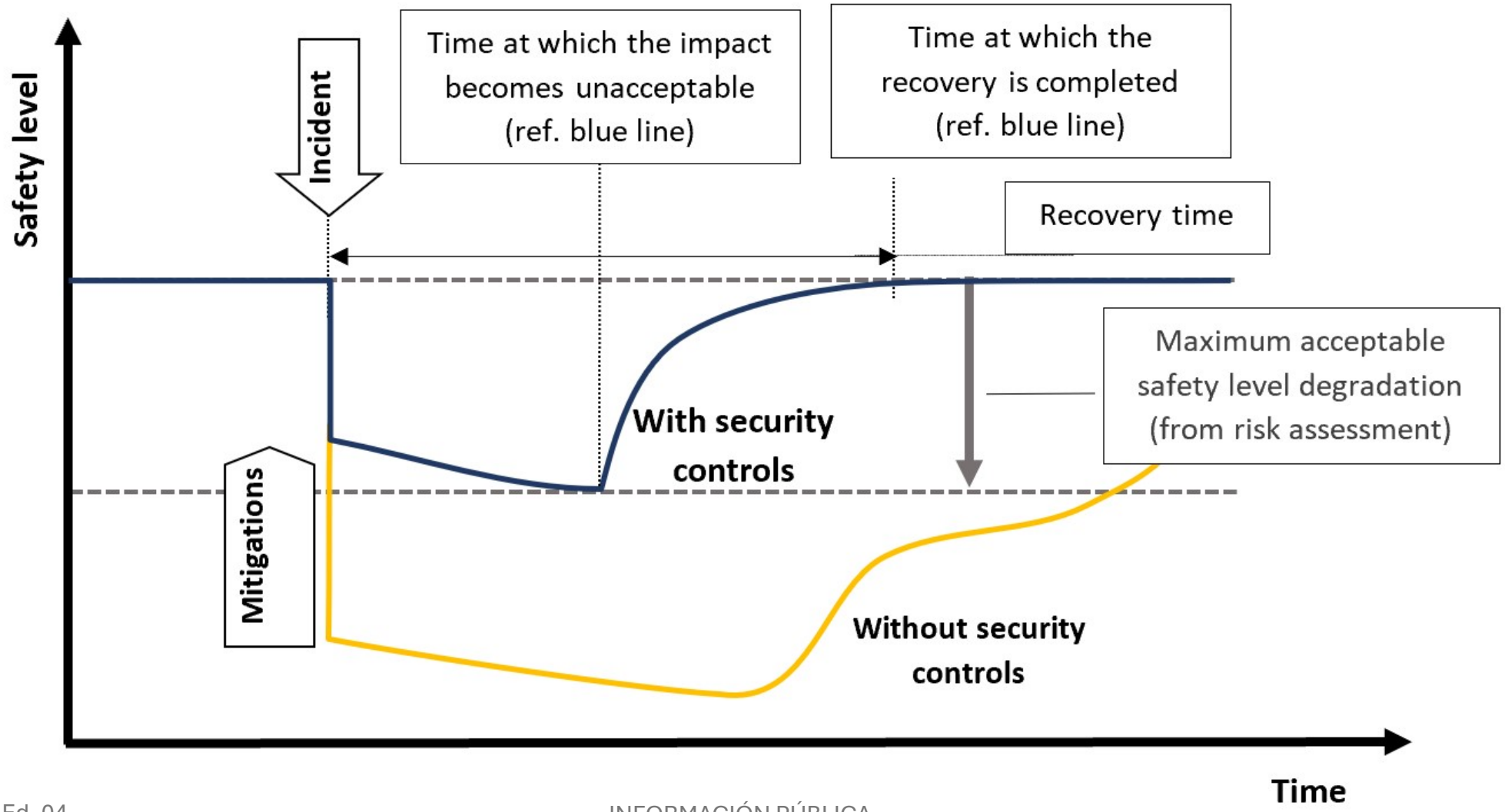
→ A systematic and well-defined approach to manage and mitigate risks and vulnerabilities.

→ The incident management process involves four stages:




→ Following a incident management process, minimizes the impact of a cybersecurity incident and quickly resumes normal operations.

## Gestión de incidentes: responder y recuperarse



# 7. Notificación interna y externa

# 7. Notificación interna y externa

## Alcance de la obligación de reporte

**Detectar**
**Responder**
**Recuperarse**

**Impacto en Safety?**

**IS.I.OR.220**

**Reg. (EU) No 376/2014**

**Reporte Externo**

**IS.I.OR.230**

**Reporte Interno**

**IS.I.OR.215**

**Autoridad Competente**

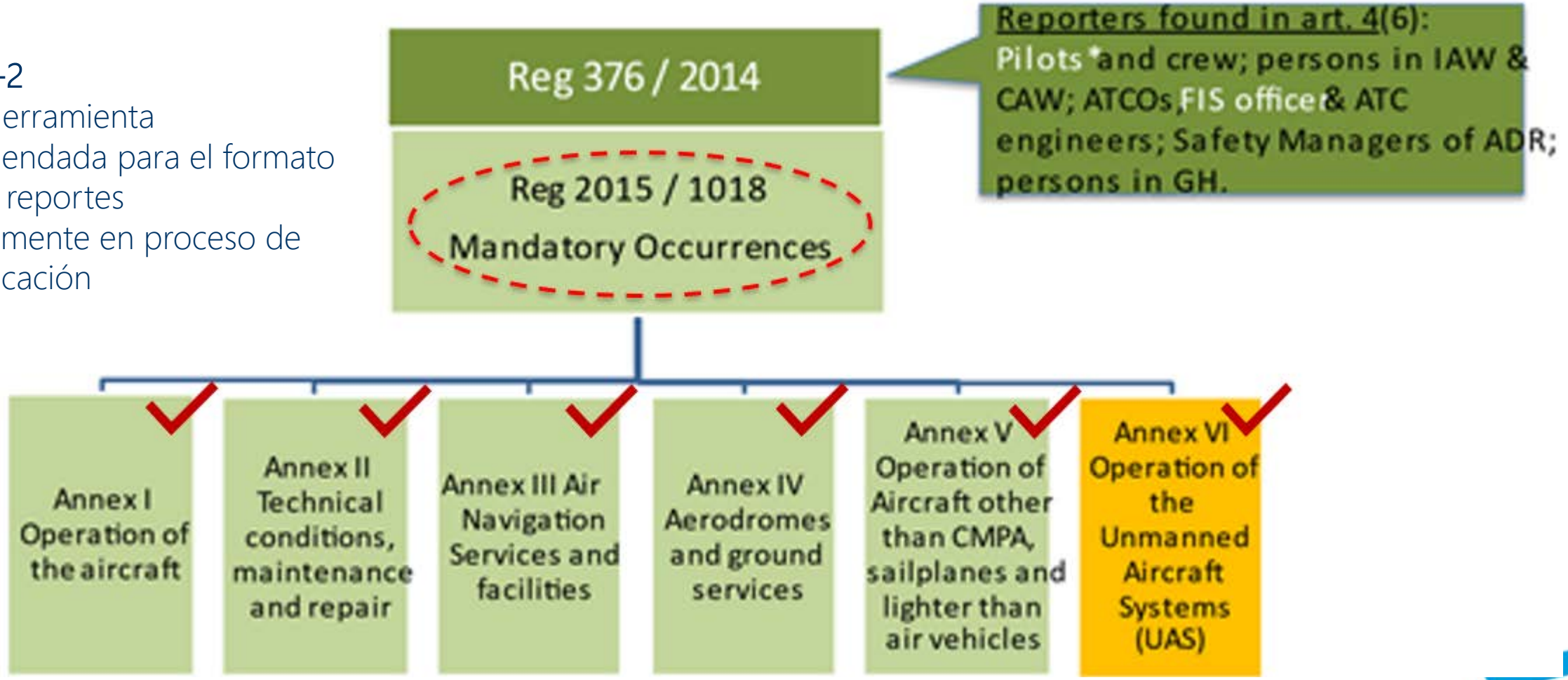
**Organizaciones de Diseño**

# 7. Notificación interna y externa

- Futura modificación del Reglamento 376/2014 y anexos del Reglamento 2015/1018

ECCAIRS-2

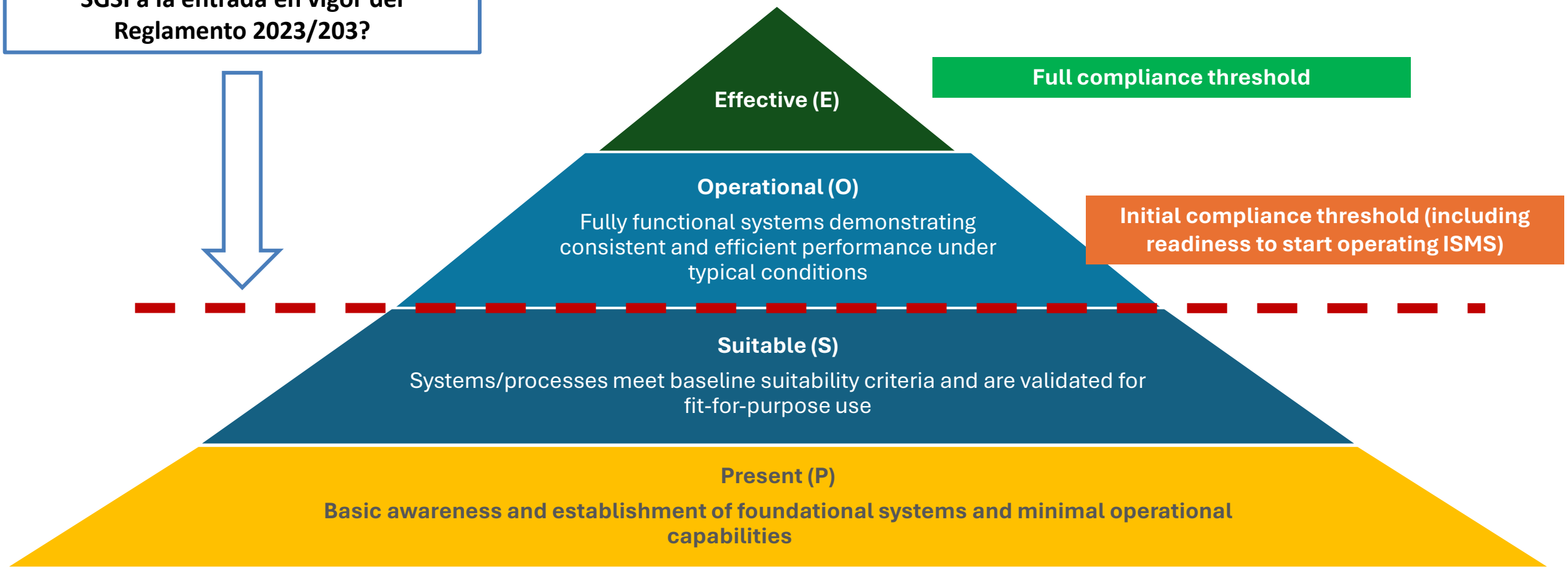
- Es la herramienta recomendada para el formato de los reportes
- Actualmente en proceso de modificación



# 8. Proceso de aprobación del SGSI

# 8. Proceso de aprobación del SGSI

**¿A qué nivel debe estar implantado el SGSI a la entrada en vigor del Reglamento 2023/203?**



# 8. Proceso de aprobación del SGSI

DSA-SG-P01-GU01 Ed. 04 Guía del Manual del Sistema de Gestión


Apéndice

Integración del Sistema de Gestión de Seguridad de la Información (SGSI)

Guía del Manual del Sistema de Gestión





DSA-SG-P01-GU02 Ed. 04 Guía de evaluación de cargos responsables


Guía Evaluación de cargos responsables del Sistema de Gestión




Otro material disponible

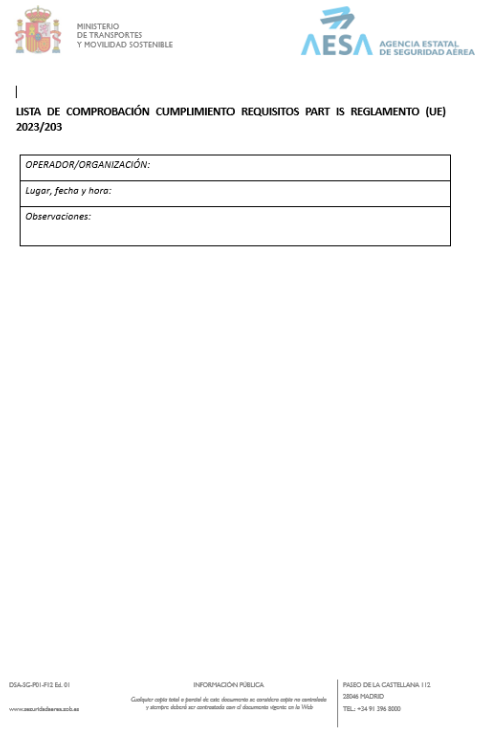
- → EASA: https://www.easa.europa.eu/en/the-agency/faqs/information-security-part
- → Autoridad Suiza (FOCA): https://www.bazl.admin.ch/bazl/en/home/flugbetrieb/security-measures/cybersecurity/part-is.html

# 8. Proceso de aprobación del SGSI

## DOCUMENTACIÓN DEL SGS/SGSI

- MGS/MGSI
- Evaluación de Riesgos
- Documentación anexa al MGS/MGSI
- Procedimiento de gestión del cambio (opcional)

DSA-SG-P01-F12 Ed. 01 Lista chequeo requisitos ISMS operadores



MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE

AESA AGENCIA ESTATAL DE SEGURIDAD AÉREA

**LISTA DE COMPROBACIÓN CUMPLIMIENTO REQUISITOS PART IS REGLAMENTO (UE) 2023/203**

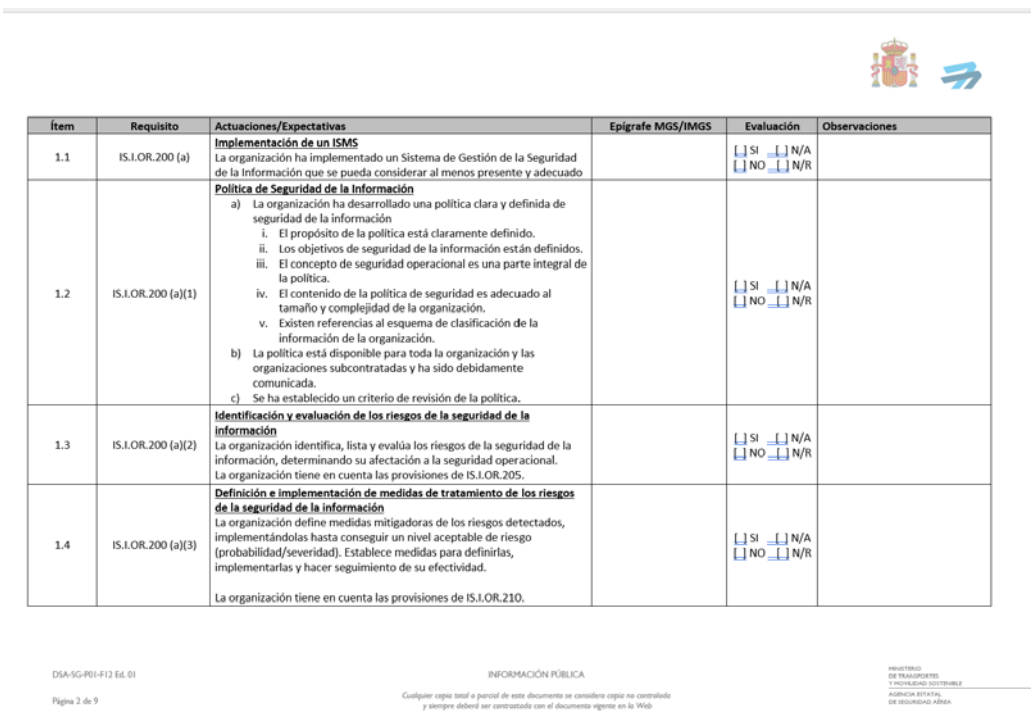
| |
|---|
| *OPERADOR/ORGANIZACIÓN:* |
| *Lugar, fecha y hora:* |
| *Observaciones:* |

DSA-SG-P01-F12 Ed. 01

INFORMACIÓN PÚBLICA

*Cualquier copia total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con el documento vigente en la Web*

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



| Ítem | Requisito | Actuaciones/Expectativas | Epígrafe MGS/IMGS | Evaluación | Observaciones |
|---|---|---|---|---|---|
| 1.1 | IS.I.OR.200 (a) | **Implementación de un ISMS**<br>La organización ha implementado un Sistema de Gestión de la Seguridad de la Información que se pueda considerar al menos presente y adecuado | | [ ] SI [ ] N/A<br>[ ] NO [ ] N/R | |
| 1.2 | IS.I.OR.200 (a)(1) | **Política de Seguridad de la Información**<br>a) La organización ha desarrollado una política clara y definida de seguridad de la información<br>i. El propósito de la política está claramente definido.<br>ii. Los objetivos de seguridad de la información están definidos.<br>iii. El concepto de seguridad operacional es una parte integral de la política.<br>iv. El contenido de la política de seguridad es adecuado al tamaño y complejidad de la organización.<br>v. Existen referencias al esquema de clasificación de la información de la organización.<br>b) La política está disponible para toda la organización y las organizaciones subcontratadas y ha sido debidamente comunicada.<br>c) Se ha establecido un criterio de revisión de la política. | | [ ] SI [ ] N/A<br>[ ] NO [ ] N/R | |
| 1.3 | IS.I.OR.200 (a)(2) | **Identificación y evaluación de los riesgos de la seguridad de la información**<br>La organización identifica, lista y evalúa los riesgos de la seguridad de la información, determinando su afectación a la seguridad operacional.<br>La organización tiene en cuenta las provisiones de IS.I.OR.205. | | [ ] SI [ ] N/A<br>[ ] NO [ ] N/R | |
| 1.4 | IS.I.OR.200 (a)(3) | **Definición e implementación de medidas de tratamiento de los riesgos de la seguridad de la información**<br>La organización define medidas mitigadoras de los riesgos detectados, implementándolas hasta conseguir un nivel aceptable de riesgo (probabilidad/severidad). Establece medidas para definirlas, implementarlas y hacer seguimiento de su efectividad.<br><br>La organización tiene en cuenta las provisiones de IS.I.OR.210. | | [ ] SI [ ] N/A<br>[ ] NO [ ] N/R | |

DSA-SG-P01-F12 Ed. 01

Página 2 de 9

INFORMACIÓN PÚBLICA

*Cualquier copia total o parcial de este documento se considera copia no controlada y siempre deberá ser contrastada con el documento vigente en la Web*

MINISTERIO DE TRANSPORTES Y MOVILIDAD SOSTENIBLE
AGENCIA ESTATAL DE SEGURIDAD AÉREA

OPS-AOC-P01-F001 Ed.0X Solicitud aprobación AOC → **En proceso de modificación para incluir las particularidades del SGSI**

# 8. Proceso de aprobación del SGSI

## AESA

Aprobación del MGSI

Aprobación del procedimiento de gestión del cambio

Supervisión de cumplimiento de los requisitos Part IS

Febrero 2026

Auditoría

Hasta la fecha de aplicabilidad → Plan de Vigilancia Continuada → Plan de Vigilancia Continuada

## Operador

Presentación de:

- MGS/MGSI
- Evaluación de Riesgos
- Documentación anexa al MGS/MGSI
- Procedimiento de gestión del cambio (opcional)
- Lista chequeo requisitos ISMS operadores
- Formato F01 (una vez modificado y publicado por AESA)

# Gracias por su atención

www.seguridadaerea.gob.es