

**EU-Latin America and Caribbean  
Aviation Partnership Project (EU-LAC APP)**

*Enhancing the aviation partnership between the EU and  
Latin America and the Caribbean*

# Un enfoque integral de los riesgos de CIBERSEGURIDAD en aviación: La estrategia Europea

**Webinar 08 Diciembre 2020**

**Juan ANTON**

**Manager Sección de Ciberseguridad en  
Aviación y Riesgos Emergentes de EASA**

**Your safety is our mission.**

# Contenido de la Presentación

## **Riesgos de ciberseguridad: factores específicos**

- La Aviación como “Sistema de Sistemas”
- El concepto de “Intencionalidad”
- Riesgos en constante evolución y de rápida propagación

## **La creación de plataformas regionales y la experiencia europea**

- Involucrar a todas las partes afectadas
- Desarrollar una estrategia de ciberseguridad a nivel europeo.
- Establecer una coordinación global
- Crear un marco normativo para la aviación, consistente con otras normativas ya existentes
- Facilitar la coordinación entre diferentes autoridades dentro de cada Estado
- Promocionar y facilitar la colaboración y el intercambio de información

## **El marco normativo**

- Tratar los riesgos de ciberseguridad durante la certificación de productos (aeronaves, motores...)
- Tratar los riesgos de ciberseguridad a nivel organizativo
- Tratar los riesgos de ciberseguridad al nivel de la supervisión nacional

## **Conclusiones**

## **RIESGOS DE CIBERSEGURIDAD: FACTORES ESPECÍFICOS**

- **LA AVIACIÓN COMO “SISTEMA DE SISTEMAS”**
- **EL CONCEPTO DE “INTENCIONALIDAD”**
- **RIESGOS EN CONSTANTE EVOLUCIÓN Y DE RÁPIDA PROPAGACIÓN**

# Riesgos de ciberseguridad: factores específicos

**La aviación es un “Sistema de Sistemas”**, que afecta a todos los sectores de la aviación, y donde los productos, servicios y organizaciones son cada vez más complejos y están cada vez más interconectados.

**Los riesgos de ciberseguridad están ligados al concepto de “intencionalidad”**, donde las vulnerabilidades son explotadas y un accidente ya no es un suceso fortuito.

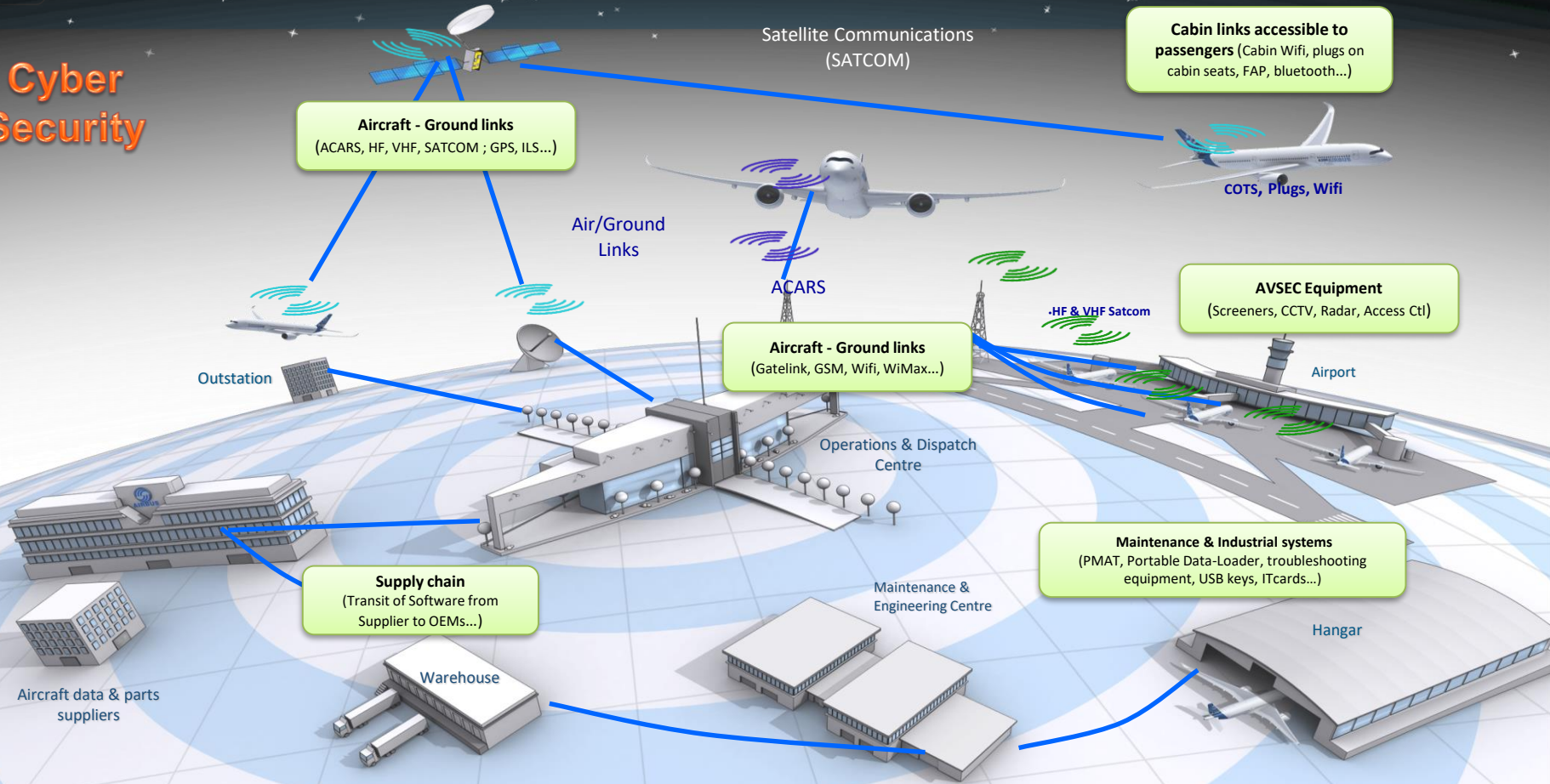
Las barreras de protección tradicionales ya no son suficientes.

**Los riesgos de ciberseguridad evolucionan muy rápidamente y los incidentes se transmiten a gran velocidad.** Esto requiere que la industria y las autoridades actúen de un modo diferente.

# LA AVIACIÓN COMO “SISTEMA DE SISTEMAS”

# Aviation is a System-of-Systems

Cyber Security



# Consideraciones importantes

- Sistemas cada vez más complejos e interconectados.
- Multitud de rutas de ataque que pueden crear un problema de protección aérea (“aviation safety”). No sólo atacando directamente a la aeronave, sino atacando a la red de navegación y tráfico aéreo. **Ejemplos:**
  - **En el fabricante:** manipulación de software, denegación de distribución de cajas de software, modificación de ICAs (Instrucciones de Aeronavegabilidad Continuada)...
  - **En la aerolínea:** corrupción de datos de mantenimiento (e.g. components de vida limitada), manipulación de “Electronic Flight Bags, EFB’s” ...
  - **En el centro de mantenimiento:** manipulación en la descarga del software...
  - Corrupción de datos de navegación...
- Los riesgos de una organización afectan a otras organizaciones. No es posible afrontar estos riesgos por uno mismo y de forma aislada. Hay que coordinar con otras organizaciones.
- Es esencial afrontar los riesgos tanto al nivel del producto (aeronave...) como al nivel de la organización.
- Es esencial establecer una coordinación nacional, regional y global.

# EL CONCEPTO DE “INTENCIONALIDAD”



# El concepto de “Intencionalidad”

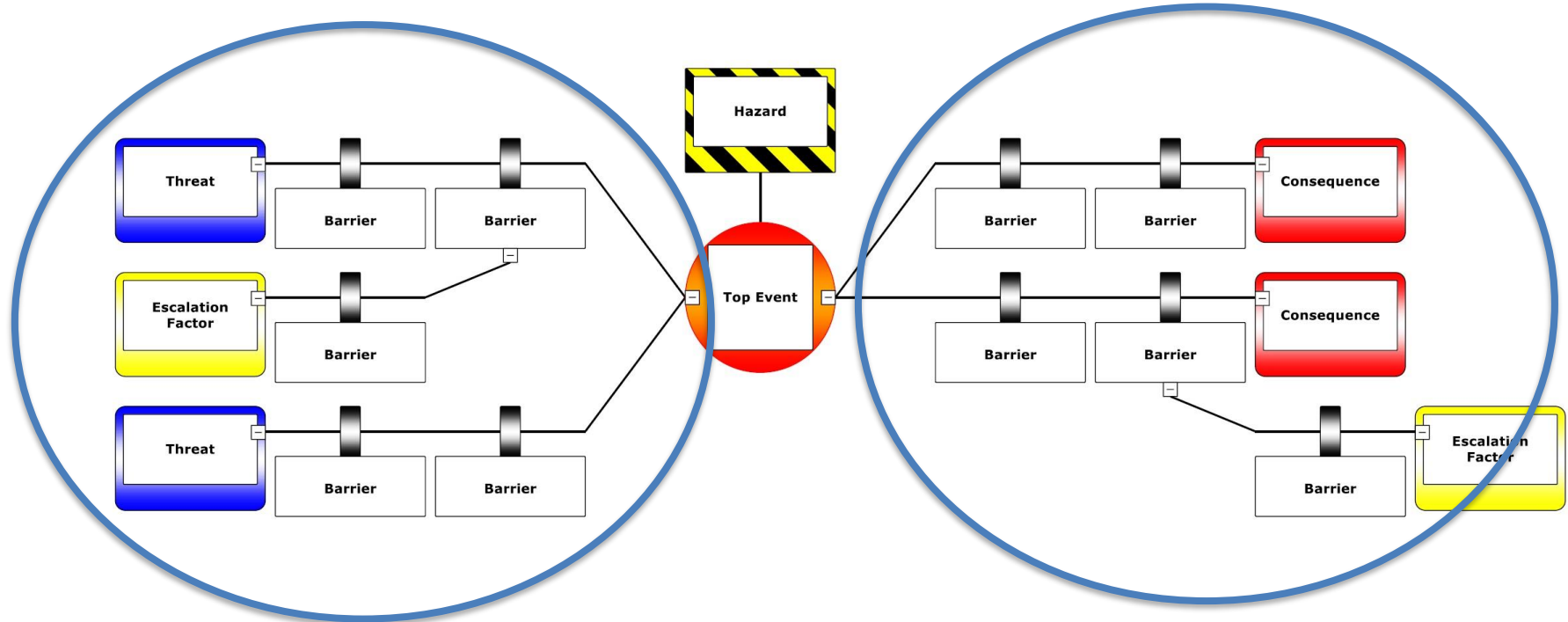
## Protección aérea tradicional



## Ciberseguridad



# Esencial coordinar “aviation safety” y “aviation security”



**AVIATION SECURITY MEASURES**  
(Medidas de seguridad aérea)

**AVIATION SAFETY MEASURES**  
(Medidas de protección aérea)

# **RIESGOS EN CONSTANTE EVOLUCIÓN Y DE RÁPIDA PROPAGACIÓN**

# Consideraciones importantes

- El intercambio de información tiene un papel fundamental en la prevención de incidentes y en evitar la propagación de aquellos que ya han tenido lugar.
- Fundamental establecer un entorno y nivel de confianza adecuados que permitan el intercambio y análisis de dicha información de manera segura y confidencial.
- Fundamental establecer una coordinación entre las diferentes autoridades del país (CAA, Agencias de ciberseguridad, Ministerios del gobierno, etc) con el objetivo de:
  - Tener en cuenta las diferentes perspectivas (seguridad aérea, protección aérea, continuidad de servicios esenciales e infraestructura crítica, etc).
  - Aumentar la armonización y compatibilidad de normativas, políticas de implementación, regímenes de supervisión (“oversight”) y reporte de incidentes.
  - Reducir la duplicación de actividades de supervisión y otras trabas administrativas.
- Las normativas y políticas de ciberseguridad deben:
  - Estar basadas en el rendimiento y en los riesgos (“performance and risk based”).
  - Ser lo suficientemente flexibles como para no tener que ser modificadas frecuentemente.
  - Ser complementadas con el desarrollo de material guía y “Estandars Internacionales”.

# **LA CREACIÓN DE PLATAFORMAS REGIONALES Y LA EXPERIENCIA EUROPEA**

- **INVOLUCRAR A TODAS LAS PARTES AFECTADAS**
- **DESARROLLAR UNA ESTRATEGIA DE CIBERSEGURIDAD A NIVEL EUROPEO.**
- **ESTABLECER UNA COORDINACIÓN GLOBAL**
- **CREAR UN MARCO NORMATIVO PARA LA AVIACIÓN, CONSISTENTE CON OTROS NORMATIVAS YA EXISTENTES**
- **FACILITAR LA COORDINACIÓN ENTRE DIFERENTES AUTORIDADES DENTRO DE CADA ESTADO**
- **PROMOCIONAR Y FACILITAR LA COLABORACIÓN Y EL INTERCAMBIO DE INFORMACIÓN**

# **LA CREACIÓN DE PLATAFORMAS REGIONALES Y LA EXPERIENCIA EUROPEA**

# EASA y la ciberseguridad

- EASA ha estado involucrada en ciberseguridad desde su creación (2003):
  - Inicialmente sólo en temas de certificación de aeronaves y motores.
  - Más tarde (desde 2011), con la introducción de ciertos requisitos de ciberseguridad para las organizaciones involucradas en *navegación y tráfico aéreo y en la operación de aeropuertos*.
- En Mayo 2015, la Comisión Europea encargó a EASA el desarrollo de un plan de acción con el fin de:
  - Desarrollar una defensa coordinada contra las amenazas de ciberseguridad.
  - Minimizar la duplicación y lagunas en el marco normativo.

Como resultado, EASA empezó el desarrollo de una *“Estrategia Integral de Ciberseguridad en Aviación”* en coordinación con las Instituciones Europeas, sus Agencias, los Estados Miembros y la Industria.

# **INVOLUCRAR A TODAS LAS PARTES AFECTADAS**



# La “European Strategic Coordination Platform” (ESCP)

## → Miembros:

- La Comisión Europea
- Otras organizaciones y agencias de la Unión Europea (*EEAS, EUROPOL, EASA, ENISA, CERT-EU, EUROCONTROL, SESAR*)
- La Agencia Europea de Defensa (EDA)
- Los estados europeos
- Las asociaciones relevantes de la Industria europea: *Fabricantes de aeronaves/motores (ASD), Líneas Aéreas (A4E, IATA, ERAA), Operadores de Helicópteros (EHA), Aeropuertos (ACI), Servicios de Navegación Aérea (CANSO), Tripulantes y personal de mantenimiento (ECA, ETF), Organizaciones de mantenimiento (EIMG), Aviación General (GAMA).*

## → Observadores:

- OACI, FAA, TCCA, Israel CAA, AIA (Fabricantes de USA), AIAC (Fabricantes de Canadá), NATO, A-ISAC (Aviation - Information Sharing and Analysis Center), EBAA (European Business Aviation Association)

# La “European Strategic Coordination Platform” (ESCP)

- **ESCP se ha estado reuniendo desde 2017.**
- **Temas de discusión:**
  - Desarrollo de una estrategia de ciberseguridad y un plan de acción para la aviación europea.
  - La coordinación de esta estrategia a nivel global.
  - El desarrollo de un marco normativo para la gestión de los riesgos de ciberseguridad.
  - El desarrollo de metodologías comunes para la evaluación de los riesgos en diferentes organizaciones.

# **DESARROLLAR UNA ESTRATEGIA DE CIBERSEGURIDAD A NIVEL EUROPEO.**

# La estrategia de ciberseguridad europea

- Desarrollada en coordinación con la ESCP, publicada por EASA el 10 de Septiembre de 2019 y alineada con la estrategia global desarrollada por OACI.
- De acuerdo con esta estrategia europea, la aviación del futuro necesita ser:
  - **Un entorno confiable**, donde las diferentes organizaciones puedan confiar en los servicios y la información prestados por otros.
  - **Un “Sistema de Sistemas” capaz de adaptarse y de soportar nuevas amenazas sin interrupciones significativas**, con un enfoque sistémico, incluyendo tanto los sistemas nuevos como los ya existentes (“legacy”).
- **Dicho esfuerzo se enfoca en dos aspectos:**
  - **Hacer de la Aviación un sistema evolutivo y ciber-resiliente**, el cual, cuando sea atacado, pueda mantener sus funcionalidades esenciales.
  - **Hacer de la Aviación un sistema que se fortalezca a sí mismo**, incorporando mecanismos de “built-in-security” desde la concepción de los correspondientes sistemas.

# **ESTABLECER UNA COORDINACIÓN GLOBAL**

# Armonización y coordinación internacional

## OACI SSGC (Secretariat Study Group on Cybersecurity)

- Grupo de coordinación de todas las actividades de ciberseguridad de OACI.
- Una de las actividades ha sido el desarrollo de una estrategia y plan de acción globales.
  - Miembros de EASA y de ESCP han participado en su desarrollo.

## OACI TFSG (Trust Framework Study Group)

- Desarrollo de un concepto de operaciones para un “International Aviation Trust Framework” (IATF).  
OBJECTIVO:
  - Establecer entidades digitales y un marco de confianza que permita el intercambio de información entre sistemas de un modo seguro e interoperativo.

# **CREAR UN MARCO NORMATIVO PARA LA AVIACIÓN, CONSISTENTE CON OTROS NORMATIVAS YA EXISTENTES**

## Normas comunes para la gestión de los riesgos de ciberseguridad:

- Desarrollo de requisitos para “Sistemas de Gestión de la Seguridad de la Información” (Information Security Management Systems, ISMS) y para reporte de incidentes de ciberseguridad.
- Aplicables a todos los sectores de la aviación y a sus interfaces, así como a las autoridades competentes.
- Con la posibilidad de integrar el ISMS en otros sistemas de gestión ya implementados por las organizaciones (SMS, SeMS...)
- Consistentes con otros requisitos de ciberseguridad europeos ya existentes (Directiva Europea 2016/1148 para servicios esenciales y Normativa Europea 2015/1998 de seguridad en aeropuertos)



# **FACILITAR LA COORDINACIÓN ENTRE DIFERENTES AUTORIDADES DENTRO DE CADA ESTADO**

# Coordinación entre autoridades dentro de los Estados Miembros

## → Esencial por los siguientes motivos:

- La ciberseguridad está justo en el interfaz entre la seguridad y la protección de la aviación (security & safety).
  - En la mayoría de países **existen diferentes autoridades responsables for “safety” and “security”**:
    - CAAs, Agencias de Ciberseguridad, Ministerios del Gobierno, etc.
  - **Cada país está afectado por varios marcos normativos que incluyen requisitos de ciberseguridad, con posibles autoridades diferentes para cada uno de ellos:**
    - Directiva Europea 2016/1148 (continuidad de servicios esenciales)
    - Normativa Europea 2015/1998 (seguridad en aeropuertos)
    - Las futuras normas de ciberseguridad de EASA (en desarrollo)
- Es importante alinear los requisitos normativos y los regimenes de supervisión.**

# **PROMOCIONAR Y FACILITAR LA COLABORACIÓN Y EL INTERCAMBIO DE INFORMACIÓN**

# Colaboración e intercambio de información

## ECCSA (European Centre for Cybersecurity in Aviation)

### → **Objetivos:**

- Promocionar el intercambio de información entre sus miembros (organizaciones y autoridades), creando una cultura de ciberseguridad y un entorno de confianza.
- Aumentar el entendimiento de los riesgos y amenazas, y la conciencia situacional global.
- **En colaboración con CERT-EU (“Computer Emergency Response Team” de las Instituciones Europeas)**
- **Actualmente tiene 30 miembros de distintos sectores de la industria y autoridades.**

## **EL MARCO NORMATIVO**

- **TRATAR LOS RIESGOS DE CIBERSEGURIDAD DURANTE LA CERTIFICACIÓN DE PRODUCTOS (AERONAVES, MOTORES...)**
- **TRATAR LOS RIESGOS DE CIBERSEGURIDAD A NIVEL ORGANIZATIVO**
- **TRATAR LOS RIESGOS DE CIBERSEGURIDAD AL NIVEL DE LA SUPERVISIÓN NACIONAL**

## EL MARCO NORMATIVO:

**TRATAR LOS RIESGOS DE CIBERSEGURIDAD  
DURANTE LA CERTIFICACIÓN DE PRODUCTOS  
(AERONAVES, MOTORES...)**

# Certificación de productos

Desde su creación en 2003, EASA certifica productos, incluyendo los aspectos de ciberseguridad.

- Estos requisitos de ciberseguridad has sido recientemente revisados por EASA, en coordinación con la FAA, y se han incorporado en las “Certification Specifications” (CS) y en los “Acceptable Means of Compliance” (AMC) (Decisión 2020/006/R de 01 Julio 2020)



En un future cercano, EASA también certificará drones (UAS).



"Airplane" by [vizzual.com](https://www.vizzual.com) CC BY 2.0

"Helico" by [JP Sangria](#) CC BY-NC 2.0

"Jet Engine" by [Chris Hunkeler](#) CC BY-SA 2.0

# Certification Specifications (CS) y Acceptable Means of Compliance (AMC)

## CS 25.1319      Equipment, systems and network            information protection

(a) Aeroplane equipment, systems and networks, considered separately and in relation to other systems, must be protected from intentional unauthorised electronic interactions (IUEIs) that may result in adverse effects on the safety of the aeroplane. Protection must be ensured by showing that the security risks have been identified, assessed and mitigated as necessary.

(b) When required by paragraph (a), the applicant must make procedures and Instructions for Continued Airworthiness (ICA) available that ensure that the security protections of the aeroplane's equipment, systems and networks are maintained.

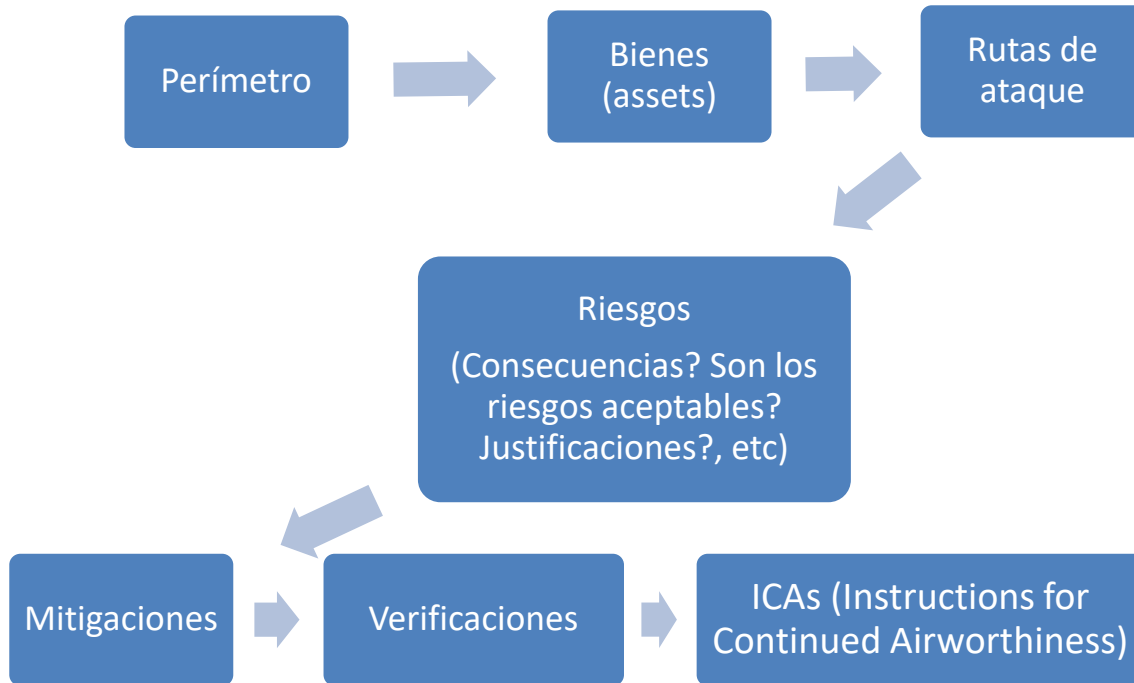
[Amdt No: 25/25]

“Mitigated as necessary” significa que el solicitante tiene la posibilidad de establecer los medios de mitigación apropiados frente a los riesgos de ciberseguridad.

AMC 20-42 proporciona medios aceptables de cumplimiento y material guía para la realización las evaluaciones de riesgo de los sistemas de información de las aeronaves.

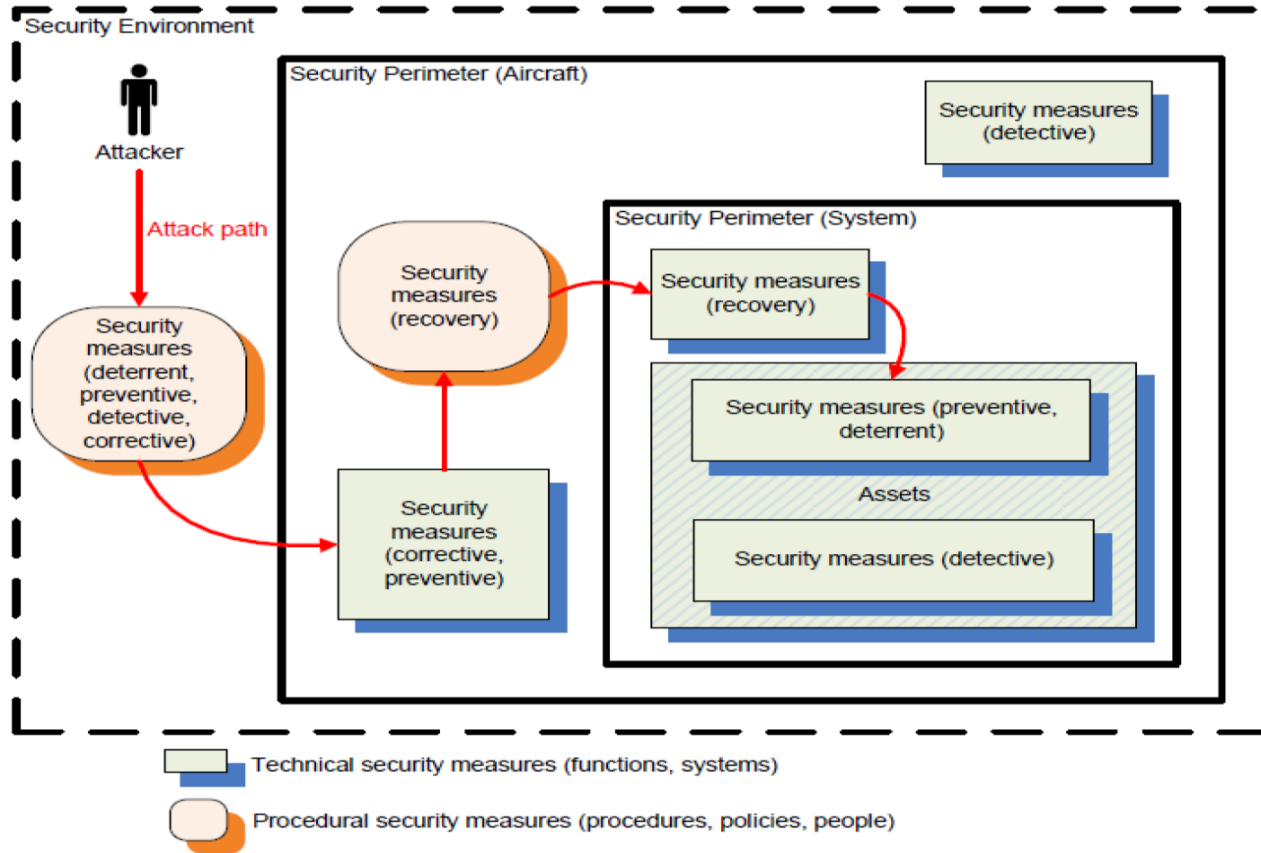


# AMC 20-42



Más detalles en Estandars  
(e.g.ED-202A, ED-203A y ED-204)

# Perímetro de seguridad



Source: ED-202A

# Rutas de ataque

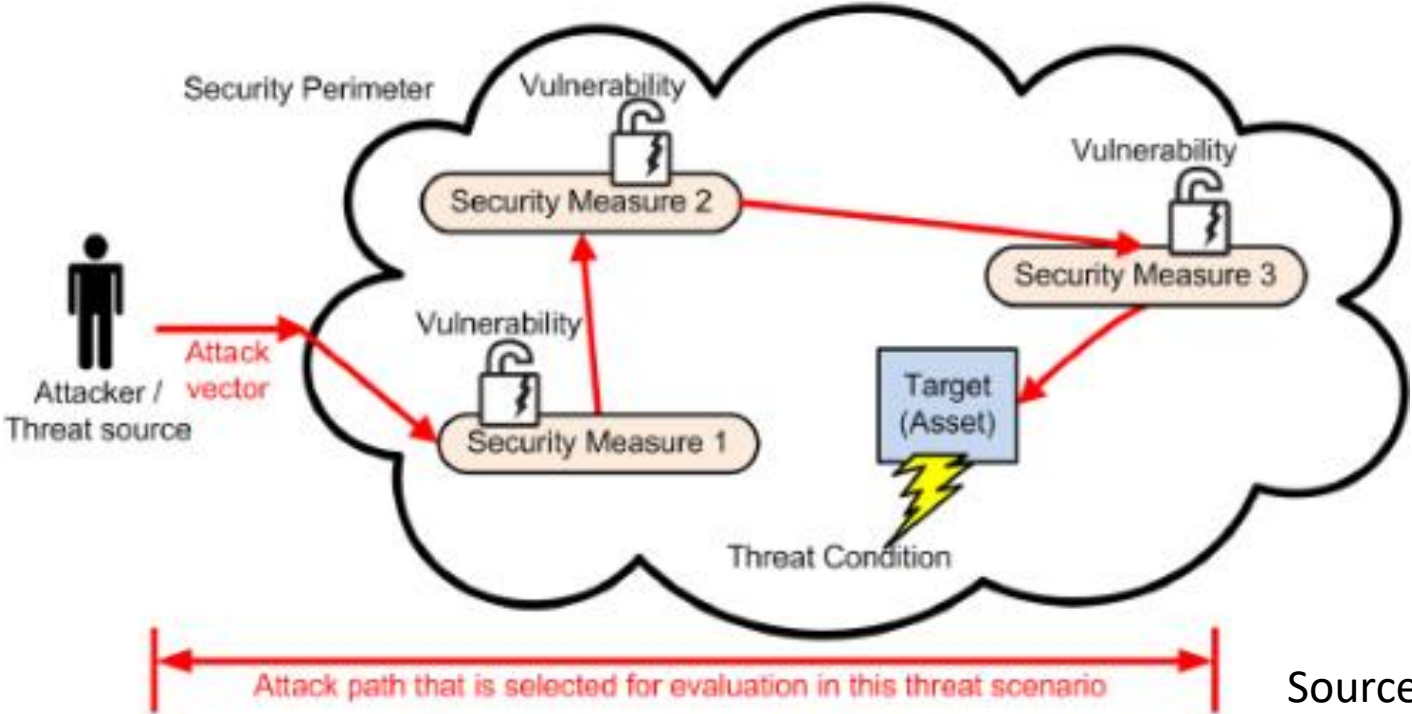


FIGURE 3-4: THREAT SCENARIO EXAMPLE 1

Source: ED-202A

# Preguntas básicas relativas a las rutas de ataque

- Tiene el sistema acceso de escritura a través de conexiones internas a uno o más sistemas de abordó ?
- Tiene el sistema servicios de conectividad externa no confiables, incluyendo centros de operaciones de las aerolíneas, equipo de mantenimiento, o conexiones inalámbricas ?
- Tiene el sistema conexiones internas bidireccionales a otros sistemas o sub-sistemas ?

# Aceptabilidad de riesgos

- Material existente en Estandars Internacionales
- Puede ser adaptado a diferentes productos

**TABLE 2-2: AIRWORTHINESS RISK ACCEPTABILITY MATRIX**

<u>Level of Threat</u>	<u>Severity of the Threat Condition Effect</u>				
	No Safety Effect	Minor	Major	Hazardous	Catastrophic
Very High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
High	Acceptable	Acceptable	Unacceptable	Unacceptable	Unacceptable
Moderate	Acceptable	Acceptable	Acceptable	Unacceptable	Unacceptable
Low	Acceptable	Acceptable	Acceptable	Acceptable	Unacceptable
Extremely Low	Acceptable	Acceptable	Acceptable	Acceptable	Acceptable*

# Mitigaciones

- Are they commensurate with the threat?
- Are they efficient?
- Which assurance do I have that the system is protected?

**TABLE 4-4: SECURITY ASSURANCE RELATION TO THREAT CONDITION SEVERITY**

Threat Condition Effect Severity	Minimum Security Assurance
Catastrophic	SAL 3 + SAL 2
Hazardous	SAL 3
Major	SAL 2
Minor	SAL 0
No Safety Effect	SAL 0

**TABLE A-1: SECURITY SPECIFIC ASSURANCE OBJECTIVES ALLOCATION TABLE**

Ref.	Objective	Scope	SAL				Security specific	Document sections
			3	2	1	0		
<b>Security Risk Assessment Objectives</b>								
O1.1	The security scope is established and validated.	AC, S	R	R	R	R	yes	4.1.1, B.2.1
O1.2	The Threat Condition Identification and Evaluation is complete and validated.	AC, S	R*	R	R	R	yes	4.1.1, B.2.1
O1.3	The Preliminary Aircraft/System Security Risk Assessments and Aircraft/System Security Risk Assessments are performed and consistent with related aircraft/system safety assessments.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1
O1.4	Preliminary Aircraft/System Security Risk Assessment results have been processed to define aircraft/system security architecture and identify the need for security measures.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1
O1.5	Aircraft/System Security Risk Assessment is consistent and complete with respect to security scope, security guidance, security requirements, security verification, security refutation and vulnerability identification.	AC, S	R*	R	A	N	yes	4.1.1, B.2.1

Source: ED-203A

**EL MARCO NORMATIVO:**  
**TRATAR LOS RIESGOS DE CIBERSEGURIDAD A**  
**NIVEL ORGANIZATIVO**

# Gestión de riesgos de ciberseguridad

**EASA está desarrollando requisitos de gestión de riesgos de seguridad de la información (Rulemaking Task RMT.0720, Part-IS)**

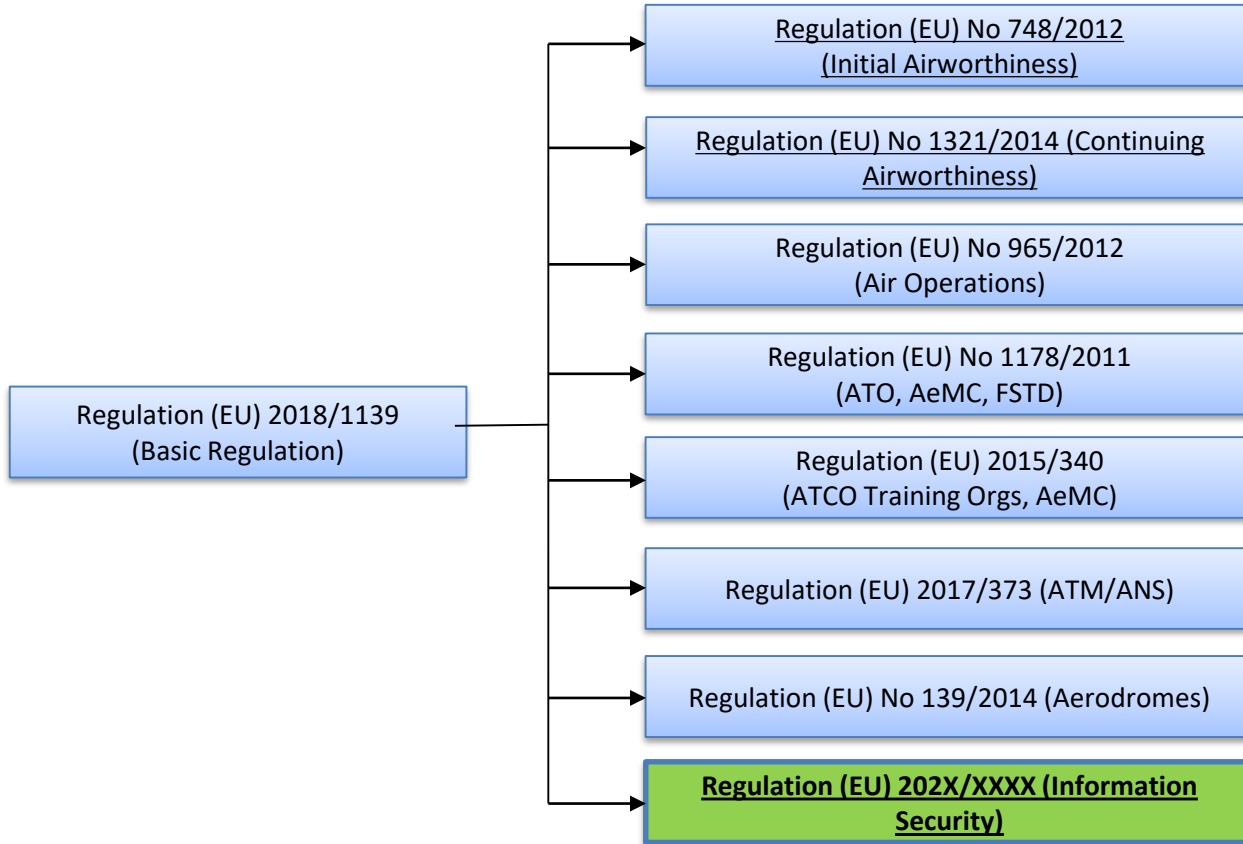
- Requisitos relativos a Information Security Management Systems (ISMS) y reporte de incidentes de ciberseguridad
- Aplicables a organizaciones en todos los sectores de la aviación, y aplicables a autoridades competentes (nivel uniforme de protección y campo de juego nivelado entre competidores)
- Incluye la posibilidad de integrar el ISMS en otros sistemas de gestión ya implementados por las organizaciones (e.g. Safety Management Systems, Security Management Systems...).



# Los riesgos de ciberseguridad afectan a todas las organizaciones

- Autoridades competentes.
- Part-21: POA (Organizaciones de Producción) y DOA (Organizaciones de Diseño)
- Part-145: Organizaciones de Mantenimiento.
- Part-CAMO: Organizaciones de Gestión de la Aeronavegabilidad Continuada
- Part-ORO: Operadores Aéreos
- Organizaciones de entrenamiento y centros médicos para tripulantes (aircrew)
- Organizaciones de entrenamiento y centros médicos para Controladores Aéreos
- Proveedores de navegación y tráfico aéreo (ATS, MET, AIS, DAT, CNS, ATFM and ASM providers and the Network Manager).
- Operadores de aeropuertos y proveedores de servicios de gestión de plataforma (rampa)

# La futura norma de ciberseguridad en el marco de EASA



# Referencias cruzadas en las normas actuales

- Un ejemplo: Normativa (EU) No 965/2012 relativa a “Operaciones Aéreas”
  
- Part-ORO (Organization Requirements for Operations):
  - Nuevo punto ORO.SEC.110 “Information Security”

“Air operators listed under point ORO.GEN.005 shall comply with Regulation (EU) 202X/XXXX”
  
- Part-ARO (Authority Requirements for Operations):
  - Modificación del punto ARO.GEN.005 “Scope”:

This Annex, together with the requirements contained in Annex I (Part-IS.AR) to Regulation (EU) 202X/XXXX, establish the requirements for the administration and management system to be fulfilled by the Agency and the Member States for the implementation and enforcement of Regulation (EU) 2018/1139 and its Implementing and Delegated Acts regarding civil aviation air operations.

# Estructura de la futura normativa: Part-IS.AR y Part-IS.OR

## → Part-IS.AR (Authority Requirements):

- **IS.AR.100** Scope
- **IS.AR.200** Information security management
  - **IS.AR.205** Information security risk assessments
  - **IS.AR.210** Information security risk treatment
  - **IS.AR.215** Information security incidents: detection, response and recovery
  - **IS.AR.220** Continuous improvement
  - **IS.AR.225** Contracting of information security management activities
  - **IS.AR.230** Personnel requirements
  - **IS.AR.245** Record keeping
- **IS.AR.300** Allocation of certification and oversight tasks to qualified entities
- **IS.AR.400** Oversight
- **IS.AR.500** Oversight programme
- **IS.AR.600** Information to the Agency
- **IS.AR.700** Immediate reaction to an information security incident with safety impact
- **IS.AR.800** Assessment of changes to organisations
- **IS.AR.900** Findings and corrective actions

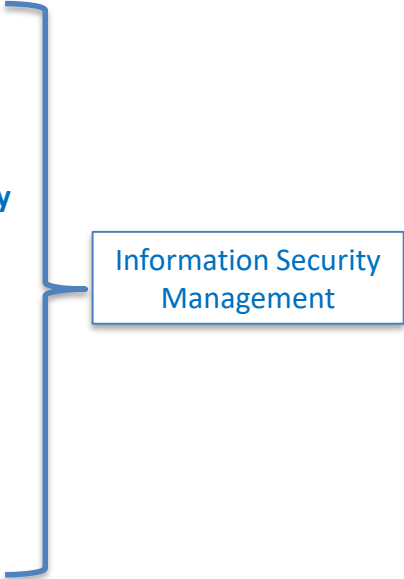
Information Security Management

Oversight of organisations

# Estructura de la futura normativa: Part-IS.AR y Part-IS.OR

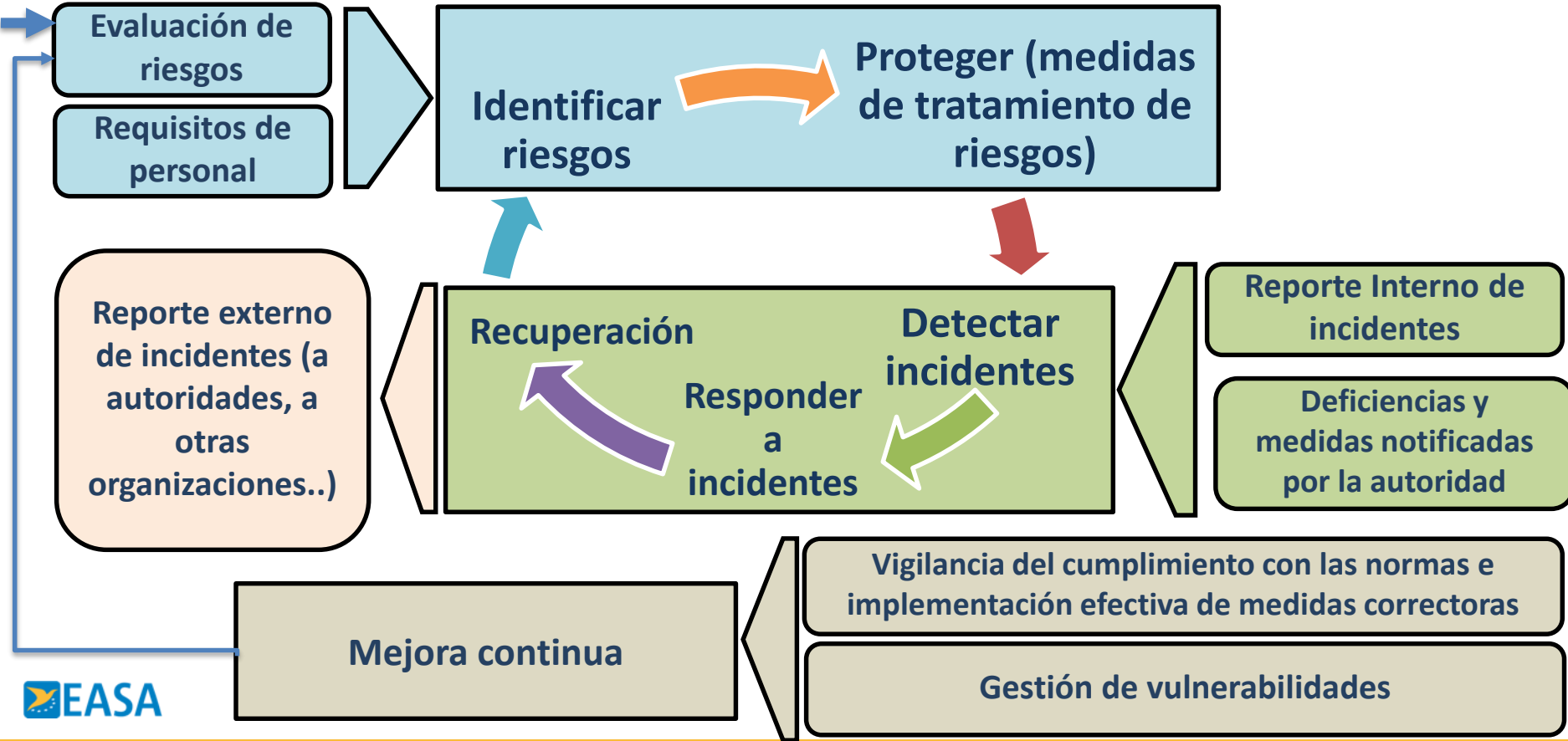
## → Part-IS.OR (Organisation Requirements):

- **IS.OR.100** Scope
- **IS.OR.200** Information security management
  - **IS.OR.205** Information security risk assessments
  - **IS.OR.210** Information security risk treatment
  - **IS.OR.215** Information security internal reporting scheme
  - **IS.OR.220** Information security incidents: detection, response and recovery
  - **IS.OR.225** Response to findings notified by the competent authority
  - **IS.OR.230** Continuous improvement
  - **IS.OR.235** Information security external reporting scheme
  - **IS.OR.240** Contracting of information security management activities
  - **IS.OR.245** Personnel requirements
  - **IS.OR.250** Record keeping
  - **IS.OR.255** Information security management manual (ISMM)
  - **IS.OR.260** Changes to the organisation



Information Security Management

# Information Security Management System (ISMS)



# Shared Trans-Organisational Risk Management (STORM)

## Principios fundamentales:

- Las organizaciones tienen que identificar los interfaces y servicios que comparten con otras organizaciones, y que pudiesen estar afectados por riesgos de ciberseguridad.
- Deben asegurar que sus evaluaciones de riesgos producen resultados que puedan ser comparados:
  - Ponerse de acuerdo en ciertas definiciones (e.g. en las categorías de riesgos, vulnerabilidades, etc)
  - Compatibilidad de las escalas de “Nivel de Amenaza” y “Severidad de Impacto”
- Deben ponerse de acuerdo en cómo compartir y qué compartir en relación a las evaluaciones de riesgo y a los riesgos mutuamente transferidos.

## Trabajo en marcha (En EASA “Acceptable Means of Compliance” y material guía, y en Estandars Internacionales, e.g. ED-201a, Joint RTCA/EUROCAE activity):

- Material guía para la identificación de interfaces entre organizaciones.
- Definición de escalas de “Severidad de Impacto” y “Nivel de Amenaza”
- Desarrollo de cláusulas para Acuerdos Externos entre organizaciones
- Desarrollo de Plantillas/Formatos con la información que podría compartirse entre organizaciones.

# Calendario de la futura normativa

- Propuesta definitiva de EASA a la Comisión Europea: Posiblemente en Abril 2021 (depende de las discusiones actualmente en marcha con la Industria y los Estados)
- Entrada en vigor: una vez adoptada por la Comisión Europea tras acordarlo con los Estados Miembros (no antes de la segunda mitad de 2022).
- Se espera que incluya medidas adicionales de transición:
  - Aplicabilidad: posiblemente alrededor de 12 meses después de la entrada en vigor.
  - Posiblemente las organizaciones tendrían otros 12 meses más para adaptar totalmente sus procedimientos, procesos, etc.



**EL MARCO NORMATIVO:**  
**TRATAR LOS RIESGOS DE CIBERSEGURIDAD AL  
NIVEL DE LA SUPERVISIÓN NACIONAL**

# Coordinación a nivel nacional

## Consideraciones fundamentales:

- **Dentro de cada Estado puede haber más de un marco normativo relativo a ciberseguridad, cada uno con diferentes objetivos:**
  - Protección (safety) de la aviación
  - Seguridad (security) de la aviación
  - Evitar la interrupción de servicios esenciales y proteger la infraestructura crítica (transporte, energía, finanzas, sanidad...)
- **Dentro de cada Estado puede haber varias autoridades, cada una responsable de un marco normativo (CAA, Agencias de ciberseguridad, Ministerios, etc).**
- **La coordinación es esencial para:**
  - Aumentar la armonización y compatibilidad de normativas y políticas de implementación.
  - Aumentar la armonización y compatibilidad de los regímenes de supervisión (“oversight”) y reporte de incidentes.
  - Reducir la duplicación de actividades de supervisión y otras trabas administrativas.

# Coordinación a nivel nacional (en la futura normativa de EASA)

- **La autoridad responsable de la futura norma de EASA sería la misma autoridad actualmente responsable de la aprobación EASA de la organización (típicamente la CAA).**
  - OBJETIVO:** Que todos los requisitos de la aprobación estén bajo el control de la misma autoridad (solo un certificado, supervisión consistente considerando la perspectiva de protección de aviación).
- **Esta autoridad podría delegar las actividades de supervisión de ciberseguridad en otra entidad (e.g. en una Agencia de Ciberseguridad nacional).**
  - OBJETIVOS:** Facilitar el acceso a personal cualificado, dar flexibilidad a los Estados para centralizar todas las tareas de supervisión de ciberseguridad para varios sectores (transporte, energía, etc).
- **Esta autoridad deberá coordinar con las autoridades responsables de las normativas de seguridad de aeropuertos y de servicios esenciales e infraestructura crítica.**
  - OBJETIVOS:**
    - Aumentar la armonización y compatibilidad de normativas, políticas de implementación, regímenes de supervisión y reporte de incidentes.
    - Reducir la duplicación de actividades de supervisión y otras trabas administrativas.
- **Las organizaciones afectadas por las otras normativas, tendrían que cumplir también con la futura norma de EASA, pero podrían usar procedimientos usados bajo las otras normativas si la autoridad considera que cumplen con los objetivos de la norma de EASA.**

# CONCLUSIONES

# Conclusiones

- Los riesgos se van incrementando exponencialmente por la digitalización y la interconexión de sistemas.
- Las barreras tradicionales de protección (en “Aviation Safety”) no son suficientes.
- Es fundamental coordinar “Aviation Security” y “Aviation Safety”.
- Hay que involucrar a todas las partes afectadas.
- Hay que coordinar las estrategias nacionales, regionales y globales.
- Es necesario establecer un marco normativo que cubra tanto los aspectos de certificación de productos y sistemas, así como los aspectos organizativos.
- Es esencial coordinar los diferentes marcos normativos (safety, security, continuation of essential services...) y de supervisión dentro de los Estados, así como a sus respectivas autoridades.
- La colaboración y el intercambio de información son esenciales.



## EU-Latin America and Caribbean Aviation Partnership Project (EU-LAC APP)

*Enhancing the aviation partnership between the EU and  
Latin America and the Caribbean*

# Muchas gracias por su atención

[www.eu-lac-app.org](http://www.eu-lac-app.org)

*This project is funded by the European Union and  
implemented by the European Aviation Safety Agency*

[easa.europa.eu/connect](http://easa.europa.eu/connect)



**Your safety is our mission.**

An Agency of the European Union 