Seminario | Modulo Jean Monnet 2025

AIR-CARE

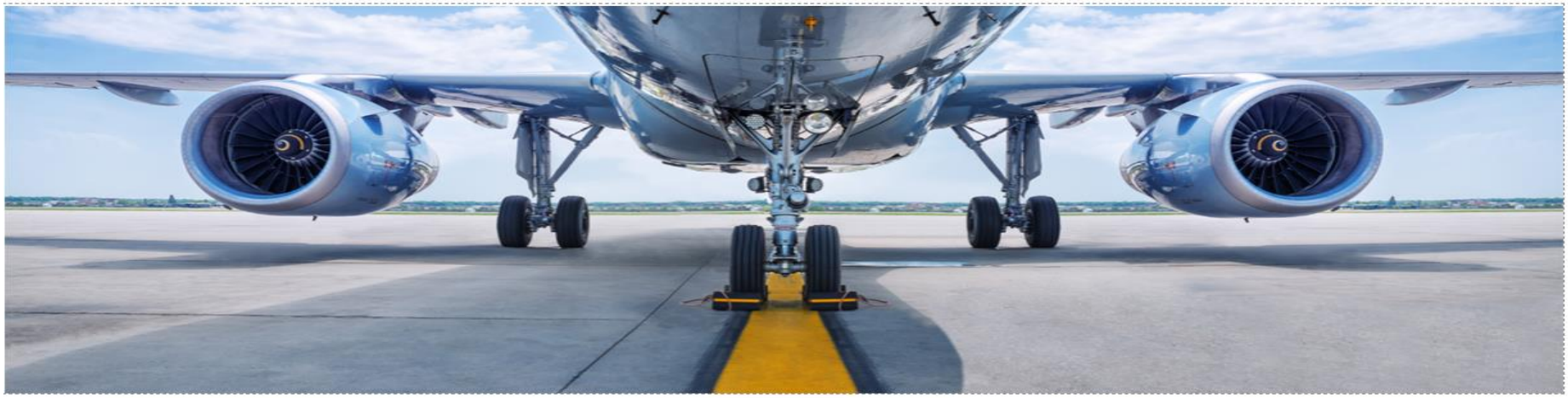
AIR transport law, Consumers And other Related issues in Europe

Project No. 101085150 - ERASMUS-JMO-2022-MODULE

Cofinanziato dall'Unione europea

Questa presentazione è stata realizzata nell'ambito del progetto AIR-CARE, finanziato dall'Unione europea. Le opinioni espresse appartengono, tuttavia, al solo o ai soli autori e non riflettono necessariamente le opinioni dell'Unione europea o dell'Agenzia esecutiva europea per l'istruzione e la cultura (EACEA). Né l'Unione europea né l'EACEA possono esserne ritenute responsabili.

This presentation has been created within the project "AIR-CARE", funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.



Ciclo di Seminari 2025

AIR-CARE AIR transport law, Consumers And other Related issues in Europe

Mercoledì 05/03/2025 | ore 9:30-13:30
Sala Galeotti UniBg (via dei Caniana, 2 Bergamo) e Online (Teams)

La Cyber-Security nel trasporto aereo: il ruolo dell'ENAC

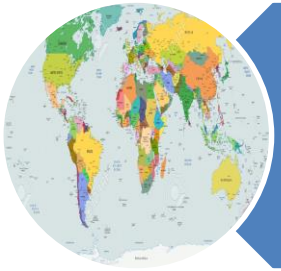
MARCO DI GIUGNO Ph.D.
DIRIGENTE ENAC
PROFESSORE A CONTRATTO UNIVERSITÀ "LA KORE"

UNIVERSITÀ DEGLI STUDI DI BERGAMO | Dipartimento di Giurisprudenza

enac Ente Nazionale per l'Aviazione Civile

SIAMO PRONTI PER QUELLO CHE POTREBBE SUCCEDERE ?

PREVENZIONE ATTRAVERSO LA NORMAZIONE



Attività dell'ICAO

Attività dell'Unione Europea
(EASA – Commissione Europea)

Attività nazionale (ENAC)

ATTIVITÀ DELL'ICAO
GLOBAL AVIATION SECURITY PLAN

ATTIVITÀ DELL'ICAO
GLOBAL AVIATION SECURITY PLAN

ICAO

Il Consiglio dell'ICAO, terza riunione della 232a sessione tenutasi il 10 giugno 2024 ha adottato la II edizione del GASEP

Doc 10118

Global Aviation Security Plan

Second Edition, 2024

ATTIVITÀ DELL'ICAO
GLOBAL AVIATION SECURITY PLAN

Nel settembre 2016, i delegati della 39^ Assemblea dell'ICAO hanno concordato sulla necessità di implementare il Piano di Sicurezza dell'Aviazione Globale (GASeP) che contiene le politiche di sicurezza dell'aviazione in un quadro di programmazione a livello globale.

Obiettivo dell'implementazione è stato quello di fornire a tutti gli stakeholder interessati alla sicurezza aerea, un piano di rafforzamento del livello della sicurezza dell'aviazione civile, indicando le azioni e gli obiettivi, da raggiungere entro il 2019, per garantire il pieno rispetto delle SARPs (Standard And Recommended Pratices) dell'Annesso 17 – Security alla Convenzione di Chicago

Nel GASEP ed. 2017 viene per la prima volta individuata la Cyber Security quale area di rischio per la sicurezza del trasporto aereo

OBIETTIVI DEL GASEP

- Migliorare la consapevolezza e la risposta al *rischio*;
- Sviluppare la *cultura della sicurezza* e la capacità umana;
- Promuovere e sviluppare il ruolo dell'*human factor*
- Migliorare le *risorse tecnologiche* e promuovere le *innovazioni*;
- Migliorare la sorveglianza e il *controllo di qualità*;
- Incrementare *cooperazione* e *supporto;*

OBIETTIVI DEL GASEP

1. Migliorare la consapevolezza del rischio e la risposta

- Sviluppare le conoscenze del personale addetto alla sorveglianza delle organizzazioni sulle tematiche generali che riguardano la cybersecurity.

- Partecipare attivamente ai gruppi di lavoro sia nazionali che internazionali al fine di acquisire un'adeguata consapevolezza su tutte le tematiche inerenti la cybersecurity con particolare riguardo alle possibili minacce.

- Assicurare il necessario e immediato scambio di informazioni con le istituzioni competenti in caso di attacchi informatici.

OBIETTIVI DEL GASEP

2. Sviluppare la cultura della sicurezza e la capacità professionale

- Pianificare e provvedere alla formazione iniziale in materia di cybersecurity tutto il personale addetto alla sorveglianza delle imprese che ricadono nei domini aeronautici di competenza ENAC.

- Provvedere a formare in modo altamente specialistico un gruppo di professionisti allo scopo di creare degli esperti di settore che potranno essere condivisi, se richiesto, con l'EASA o con altre autorità aeronautiche in base alle previsioni contenute nel regolamento (UE) 2018/1139 «Pool of European Aviation Inspectors».

OBIETTIVI DEL GASEP

3. Assicurare un livello di sorveglianza adeguato al livello del rischio / minacce

- Pianificare e monitorare i piani di sorveglianza sulle imprese certificate al fine di verificare l'adeguatezza della gestione delle situazioni di crisi, la capacità di individuare le cause all'origine e l'attuazione delle necessarie azioni correttive.

- Effettuare un riesame annuale sull'adeguatezza delle misure intraprese dall'Ente in materia di cybersecurity.

OBIETTIVI DEL GASEP

4. Migliorare la cooperazione e il supporto

- Assicurare il necessario coordinamento e scambio di informazioni con gli organismi nazionali e internazionali che si occupano di cyber security.

- Partecipare attivamente ai test di simulazione di attacchi malevoli condotti sia a livello nazionale che europeo e internazionale.

- Istituire tavoli tecnici con le organizzazioni / associazioni di settore per assicurare un proficuo scambio di informazioni tra l'industria e l'Ente al fine di individuare le criticità più rilevanti che debbono essere risolte.

ATTIVITÀ DELL'UE

SICUREZZA INFORMATICA

Safety	Security
EASA	Commissione UE - AVSEC

ATTIVITÀ DELL'UE: Reg. UE 1138/2018

Modifica al Regolamento basico istitutivo di EASA

Ampliamento delle competenze di EASA

ATTIVITÀ DELL'UE: Reg. UE 1138/2018

Modifica al Regolamento basico istitutivo di EASA

Ampliamento delle competenze di EASA: Introduzione della Cybersecurity

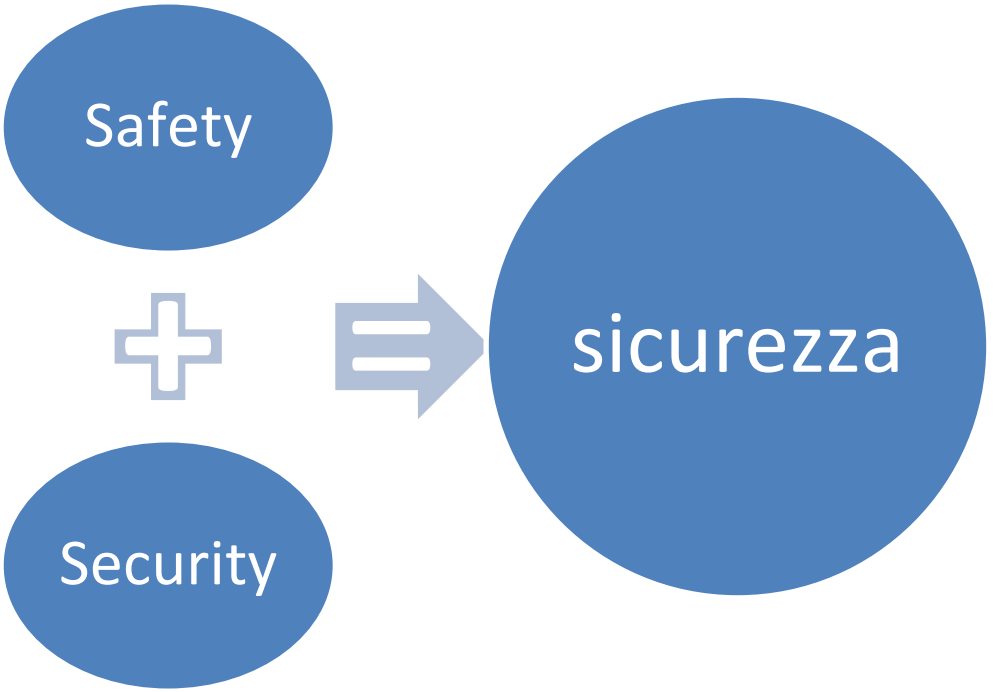
HA INTRODOTTO PER LA PRIMA VOLTA NELLA NORMATIVA EUROPEA LA NECESSITÀ DI PROTEGGERE TUTTO IL SISTEMA AVIAZIONE CIVILE DAGLI ATTACCHI INFORMATICI, DAL PROGETTO AL MANTENIMENTO DEL SISTEMA / IMPIANTO NEL CORSO DELLE OPERAZIONI.

L'INTRODUZIONE DELLA CYBER-SECURITY NEL REGOLAMENTO RICONOSCE LA CRITICITÀ DELLA MATERIA CONSIDERATO L'USO SEMPRE PIÙ ESTENSIVO DELLE NUOVE TECNOLOGIE SIA A TERRA CHE IN VOLO E ALLA POSSIBILITÀ CHE ATTACCHI INFORMATICI MALEVOLI POSSANO COMPROMETTERE LA SICUREZZA DELLE OPERAZIONI NEL SUO COMPLESSO.

ATTIVITÀ DELL'UE: Reg. UE 1138/2018

Art. 88: ***INTERDIPENDENZE TRA SICUREZZA E SECURITY NELL'AVIAZIONE CIVILE***
La Commissione e l'Agenzia e gli Stati membri cooperano in materia di security dell'aviazione civile, compresa la cybersicurezza, quando vi siano interdipendenze tra sicurezza e security nell'aviazione civile.

UN NUOVO APPROCCIO NELL'USO DELL'ESPRESSIONE SICUREZZA!



ATTIVITÀ DELL'UE:

QUADRO NORMATIVO IN MATERIA DI SECURITY

I **Regg. 300/2008** e **1998/2015** hanno stabilito le regole comuni per la sicurezza (security) dell'Aviazione Civile in ambito europeo.

Il regolamento di esecuzione (UE) **2023/203** stabilisce le norme per l'identificazione e la gestione dei rischi per la sicurezza delle informazioni nelle organizzazioni aeronautiche e nelle autorità aeronautiche competenti, tra cui l'EASA. Questo regolamento segue il regolamento delegato (UE) **2022/1645** pubblicato il 23 settembre 2022, applicabile alle organizzazioni di progettazione e produzione approvate, nonché ai gestori di aeroporti e ai fornitori di servizi di gestione del piazzale.

ATTIVITÀ DELL'UE:

QUADRO NORMATIVO IN MATERIA DI SECURITY

DISPOSIZIONI ATTUATIVE DEI REGG. (UE) 2023/203 E 2022/1645

Nel mondo interconnesso dell'aviazione, i rischi per la sicurezza delle informazioni non sono limitati solo al livello del prodotto. L'aviazione è un "sistema di sistemi" che comprende, insieme ai prodotti aeronautici e alle relative tecnologie, persone, processi e altri asset immateriali che sono a loro volta vulnerabili alle minacce per la sicurezza

OBIETTIVO DELLA UE

Predisporre un **piano per la cybersecurity** che preveda di istituire un centro comune che sviluppi difese specifiche per l'industria dell'aviazione. La strategia fisserà standard comuni e iniziative congiunte per sventare le minacce della rete. Infine, EASA collaborerà con l'Agenzia europea per la sicurezza informatica (ENISA) per tradurre in pratica le indicazioni delle **direttive NIS** comunitaria sulla cybersecurity.

OBIETTIVO DELLA UE

- La Direttiva (UE) n. 2022/2555 c.d. NIS2 sottolinea l'importanza di rafforzare la sicurezza informatica nel settore dei trasporti per proteggere le infrastrutture critiche nei trasporti aerei, marittimi, ferroviari e stradali;
- Nell'ambito della direttiva NIS troviamo vettori aerei, enti di gestione aeroportuale, aeroporti principali ed enti che gestiscono installazioni ausiliarie contenute negli aeroporti e operatori di controllo della gestione del traffico che forniscono servizi di controllo del traffico aereo (ATC), riconosciuti come essenziali dalla direttiva NIS2 e rientranti nel perimetro della Perimetro di Sicurezza Nazionale Cibernetica (PNSC) sulla base del DPCM 15 giugno 2021.

ATTIVITÀ DELL'ENAC

ENAC è stata designata dal Governo Italiano (D.M. 21.07.09) quale unica autorità responsabile del coordinamento e del monitoraggio dell'attuazione delle norme fondamentali comuni in tema di sicurezza (security).

ENAC, quale autorità di settore, ha avviato il processo di attuazione del Global Aviation SEcurity Plan predisposto dall'ICAO

Le norme che regolano la sicurezza degli aeroporti si sono evolute sempre in risposta alla minaccia contingente, e troppo spesso solo dopo che la stessa si è manifestata.

Il ruolo dell'ENAC:

L'ENAC quale autorità di regolazione tecnica dell'aviazione civile ha la responsabilità di essere proattiva nel prevenire le nuove minacce

RISULTATI PRIORITARI ICAO E AZIONI ENAC

- Realizzare un security repository – Finanziare progetti R&D
- Individuare ed affrontare le minacce di cyber-security
- Istituire un sistema elettronico per la raccolta di segnalazioni volontarie
- Contribuire a migliorare l'innovazione e lo sviluppo tecnologico
- Implementare metodologia RBO (Risk Based Oversight) - Potenziare efficacia controlli qualità

AZIONI ENAC

FAVORIRE LO SVILUPPO DELLA SECURITY CULTURE

La **security culture** è la cultura organizzativa che:

- si basa sullo ***human factor*** e sulla ***consapevolezza del proprio ruolo***
- è influenzata da formazione, valori organizzativi, mission dell'organizzazione o dell'impresa, leadership, linguaggio di lavoro, norme, abitudini e policy, layout degli ambienti di lavoro (building layouts).
- consente di Implementare la "just culture" nelle segnalazioni di security senza timore di conseguenze negative a carico delle parti coinvolte;

AZIONI ENAC

ISTITUIRE UN SISTEMA ELETTRONICO PER LA RACCOLTA STRUTTURATA DI SEGNALAZIONI VOLONTARIE

eE-MOR

L'attuale sistema eE-MOR (electronic ENAC - Mandatory Occurrence Reporting), che consente la raccolta delle segnalazioni degli eventi aeronautici, è stato realizzato dall'ENAC per rispondere ai requisiti definiti dai Regolamenti (UE) n. 376/2014 e n. 2015/1018 sulla segnalazione di eventi nel settore dell'aviazione.

Security occurrences:

- **ALLARME BOMBA O DIROTTAMENTO**
- **DIFFICOLTÀ NEL CONTROLLARE PAX IN STATO DI UBRIACHEZZA, VIOLENTI O INDISCIPLINATI (UNRULY PASSENGERS)**
- **INDIVIDUAZIONE DI PAX CLANDESTINI**

AZIONI ENAC

REALIZZARE UN REPOSITORY PER DOCUMENTI DI SECURITY ACCESSIBILE DA PARTE DI COLORO CHE HANNO NECESSITÀ DI CONOSCERE

L'ENAC implementerà una piattaforma ICT on-line attraverso la quale condividere con gli stakeholder, in modo sistematizzato e strutturato, documentazione e normativa. Le comunicazioni garantiranno flussi informativi con meccanismi di accesso altamente sicuri.

AZIONI ENAC

SVILUPPARE LA METODOLOGIA (RBO) RISK BASED OVERSIGHT NELLA PROGRAMMAZIONE DELL'ATTIVITÀ DI CONTROLLO DELLA CONFORMITÀ

L'ENAC intende sviluppare e attuare un modello di RBO nel quale la pianificazione della sorveglianza sia guidata dall'identificazione del

LIVELLO DEL RISCHIO (funzione della natura, della complessità dell'organizzazione e dei processi svolti)	capacità di identificare e gestire i rischi dei soggetti sottoposti ad oversight

AZIONI ENAC

INDIVIDUAZIONE DEI PRINCIPALI FATTORI DI RISCHIO: CASI DI CYBER ATTACCHI NEL TRASPORTO AEREO

Nel 2016 (EASA) stimava circa **1000** cyberattacchi al mese ad aerei e aeroporti. Intrusioni e minacce che hanno provocato ritardi nelle partenze, azzeramento dei servizi o furti di dati personali.

AZIONI ENAC

INDIVIDUAZIONE DEI PRINCIPALI FATTORI DI RISCHIO

La gestione del rischio di security non può essere lasciata esclusivamente alle entità regolate, ma necessita di un quadro organico di difesa.
Non esistono solo aeroporti ed aeromobili, ma un mondo complesso che è parte integrante del sistema dell'aviazione civile e ne risulta essenziale e insostituibile

FATTORI ESTERNI
Elementi di contest da analizzare con appropriate metodologie e cooperazione con gli attori istituzionali e capacità interne

FATTORI INTERNI
Analisi delle vulnerabilità ed il ruolo della "minaccia interna"

INTERDIPENDENZE
Analisi degli impatti che minacce a soggetti esterni, non-aviation, possano arrecare ai Servizi della navigazione area

Fonte: ENAV

AZIONI ENAC

INDIVIDUAZIONE DEI PRINCIPALI FATTORI DI RISCHIO: UN FOCUS SUL C.D. RISCHIO INTERNO

Fonte: ENAV


SECURITY
PRIVACY

AEROPORTO/OPERATORE AEREO/HANDLER

GESTIONE DEI DATI PERSONALI RISPETTO LE ESIGENZE DI SECURITY CHE RICHIEDONO L'ACCESSO A DETTI DATI

Rischio:

SPROPORZIONE TRA MISURA E RISCHIO

mitigazione del rischio

Formazione e Responsabilizzazione del personale; Identificazione del responsabile

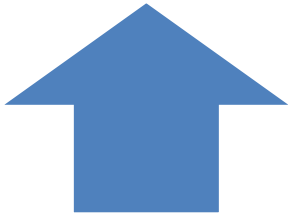
SPERIMENTAZIONE SUI DATI BIOMETRICI

qualità

COSA CI ASPETTA NEL PROSSIMO FUTURO?

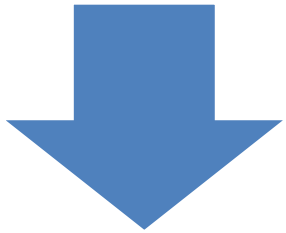
- MAGGIORE CONSAPEVOLEZZA DEL PASSEGGERO SUI PROPRI DIRITTI;
- PERSONALE SEMPRE PIÙ SPECIALIZZATO E QUALIFICATO;
- ORGANIZZAZIONE VOLTA AD INDIVIDUARE I RISCHI E LE MISURE DA ADOTTARE;

AL VERIFICARSI DI QUESTE CONDIZIONI IL PASSEGGERO POTRÀ SCEGLIERE TRA:



Velocità delle operazioni

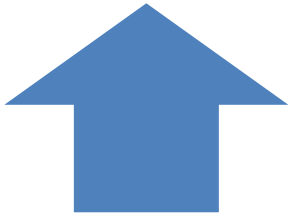
Privacy



COSA CI ASPETTA NEL PROSSIMO FUTURO?

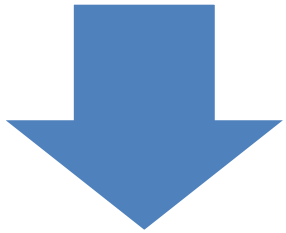
- MAGGIORE CONSAPEVOLEZZA DEL PASSEGGERO SUI PROPRI DIRITTI;
- PERSONALE SEMPRE PIÙ SPECIALIZZATO E QUALIFICATO;
- ORGANIZZAZIONE VOLTA AD INDIVIDUARE I RISCHI E LE MISURE DA ADOTTARE;

AL VERIFICARSI DI QUESTE CONDIZIONI IL PASSEGGERO POTRÀ SCEGLIERE TRA:



Velocità delle operazioni

Privacy



PER ULTERIORI INFORMAZIONI:

WWW.ENAC.GOV.IT

WWW.GARANTEPRIVACY.IT/PACCHETTOPROTEZIONEDATI

DOMANDE?

SI RINGRAZIA PER L'ATTENZIONE