Organización de Aviación Civil Internacional
Oficina Regional Sudamericana
Decimoctava Reunión de Autoridades de Aviación Civil de la Región Sudamericana (RAAC/18)
(Sao Paulo, Brasil, 24 al 26 de febrero de 2025)

RAAC/18-WP/39
06/02/25

Item 5A of Agenda: **Effectiveness in Plans**

AVIATION CYBERSECURITY STRATEGY

Working Paper presented by Colombia, *"The Country of Beauty"*

SUMMARY

Aviation is undergoing an unprecedented digital transformation. Technologies such as digital communications, intelligent system integration, data analysis, advanced surveillance, predictive ATM systems, and cloud computing are redefining the sector. However, this increasing interconnection expands the attack surface and heightens vulnerability to cyber threats. These increasingly sophisticated attacks jeopardize operational security, data privacy, and confidence in the system.

To counter this challenge, it is crucial to strengthen cybersecurity in the aviation sector. ICAO Member States must implement the ICAO Cybersecurity Strategy and Cybersecurity Action Plan, adapting them to their national contexts, while reinforcing their organizational culture, technological infrastructure, and regulatory frameworks to address the specific challenges of cybersecurity in civil aviation.

Additionally, the cross-border nature of cyberspace necessitates mechanisms for dialogue and technical and operational cooperation among Member States.

References:

- ICAO Annex 17: Aviation Security (AVSEC).
- ICAO Document: Aviation Cybersecurity Strategy.
- ICAO Document: Guidance on Cybersecurity Policy.
- ICAO Document: Resolution A41-19 on Addressing Cybersecurity in Civil Aviation.
- ICAO Document: Cybersecurity Action Plan.

ICAO Strategic Objectives	- *Operational safety.* - *Air navigation capacity and efficiency.* - *Aviation security and facilitation.* - *Every flight is safe (Safety and Security).* - *Aviation provides seamless, accessible, and reliable mobility for all.* - *No country is left behind..*

1. Introduction

1.1 In recent years, global aviation has undergone a rapid and extensive digital transformation, driven by the adoption of cloud computing, big data, system integration, and digital information management. These advancements are key to optimizing airspace utilization, enhancing safety, and improving operational efficiency. However, this expanding digital frontier also introduces significant cybersecurity challenges.

1.2 The growing interconnection of aviation systems amplifies vulnerabilities to cyberattacks, which could disrupt essential services, compromise operational security, infringe on data privacy, and erode trust in the system. Strengthening cybersecurity is essential to mitigate these risks and ensure information protection and operational continuity.

1.3 The cooperation of ICAO Member States is essential to building a resilient airspace against cyber threats**,** given the transnational nature of cyberspace**,** which requires efficient mechanisms for dialogue, technical cooperation, and operational coordination among States. Sharing information, best practices, and coordinating responses to cyber incidents are key to ensuring global civil aviation security.

1.4 This collective effort will help establish a safer and more reliable airspace for all**,** enabling a coordinated response to cybersecurity failures or incidents**,** such as the Microsoft cyberattack on July 19, 2024**,** which affected administrative systems of several airlines worldwide**.** Minimizing impact through timely coordination will ensure operational security and continuity across the aviation sector.

2. Discussion

2.1 The digital transformation has optimized aviation processes across all areas, from CNS-ATM to information systems used by airlines, airports, and regulatory authorities. However, this increased interconnection introduces new vulnerabilities, as formerly isolated systems are now integrated, creating potential entry points for cyber threats. Aviation, by nature, is a collaborative international activity that relies on constant interconnectivity between systems for flight optimization. Therefore, individual and collective cybersecurity efforts are essential to minimize risks, which range from unauthorized access to sensitive data to manipulation of critical systems, ultimately affecting operational security, business continuity, and public confidence.

2.2 ICAO recognizes cybersecurity as a shared responsibility that demands global cooperation. However, the rapid evolution of cyber threats and their borderless nature make swift action and coordinated responses essential. States must exchange information, best practices, and technical resources to address threats effectively and ensure aviation security.

2.3 The aviation sector faces the dual challenge of maintaining the benefits of digitalization while ensuring cybersecurity. This requires: Implementing advanced digital security technologies, providing continuous personnel training in cybersecurity protocols, sharing intelligence on emerging threats and vulnerabilities, developing cybersecurity policies and best practices for aviation organizations.

2.4 The cybersecurity strategy should focus on four key pillars: Personnel Training: Building technical expertise within aviation authorities and industry stakeholders. Infrastructure Security: Strengthening internal technological defenses and adopting advanced threat detection mechanisms. Regulatory Development: Establishing comprehensive legal frameworks to promote cybersecurity across the entire civil aviation sector. International Cooperation: Enhancing collaboration between aviation

entities, authorities, and private-sector partners.

2.5 With the growing integration of digital systems, cloud computing, and big data in aviation, cybersecurity must be a priority. Member States should work to secure critical aviation systems, safeguard operational data, and prevent cyberattacks that could compromise aviation security.

2.6 Aviation cybersecurity requires harmonized strategies across national jurisdictions to ensure global interoperability and effective threat mitigation. States must exchange best practices, strengthen intelligence-sharing mechanisms, and implement unified incident response protocols.

2.7 While national cybersecurity strategies should align with each country's regulatory framework, they must also be interoperable at an international level to ensure seamless and secure global aviation operations. Collaboration between civil aviation experts, regulatory authorities, and technology providers will be essential to identify vulnerabilities and enhance resilience against cyber threats.

2.8 Cybersecurity in aviation requires a global and coordinated response. ICAO, in collaboration with Member States, must lead efforts to establish a resilient cybersecurity framework that protects aviation from cyber threats. The safety of millions of passengers and the stability of the global aviation system depend on it.

3. Suggested Action

3.1 The meeting is invited to:

a) Define cybersecurity actions within the SAM Region Transformation Strategy, extending its scope to all aviation stakeholders and air traffic management systems to ensure efficient and comprehensive cybersecurity protection

- END -