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/40
06/02/25

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

STRENGTHENING CYBERSECURITY IN CIVIL AVIATION: A COLLABORATIVE WORK PLAN FOR THE PROTECTION OF CIVIL AVIATION CIVIL

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

SUMMARY

The increasing digitalization of civil aviation has led to greater vulnerability to cyberattacks, affecting both operational safety and critical sector infrastructures. These cyberattacks, which are becoming more frequent and sophisticated, pose a threat to passenger safety, flight operations, and the reputation of the industry. In this context, cybersecurity has become a strategic priority to protect navigation, communication, and flight management systems, among others. The International Civil Aviation Organization (ICAO) has developed a Cybersecurity Strategy and Action Plan to guide States and key stakeholders in implementing effective cybersecurity measures.

To address these challenges, it is essential to adopt a comprehensive and collaborative approach. This includes the creation of specific cybersecurity frameworks for civil aviation, the formation of specialized teams, and the establishment of cyber incident response centers. Additionally, international and regional cooperation among SAM Region States is crucial for enhancing coordination in combatting cross-border cyber threats. Training personnel, from operational staff to senior management, on technical and governance aspects of cybersecurity is essential to prevent and mitigate the effects of cyberattacks on civil aviation.

References

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

***ICAO Strategic Objectives**:*	***1.*** *Every Flight is Safe (Safety and Security).* ***2.*** *No Country is Left Behind.* ***3.*** *The Convention on International Civil Aviation and Other Treaties, Laws, and Regulations Address All Challenges.* ***4.*** *The Economic Development of Air Transport Ensures Economic Prosperity and Social Well-being for All.*

1. Introduction

1.1 The increasing digitalization of civil aviation has radically transformed the sector, exposing it to unprecedented cybersecurity vulnerabilities. Cyberattacks, which are becoming more sophisticated and frequent, threaten both operational safety—endangering lives on board—and civil aviation security, impacting critical infrastructure, operations, and reputation. Given this reality, strengthening cybersecurity has become a strategic imperative to ensure the sector's continuity and resilience.

1.2 ICAO, through its Aviation Cybersecurity Strategy and Cybersecurity Action Plan, has provided a solid reference framework to address these challenges. However, effective implementation of these recommendations requires coordinated and sustained action at the regional level, as well as a firm commitment from all stakeholders, including Member States, industry, and academia

2. Discussion

2.1 The growing interconnection of systems in civil aviation, driven by digitalization and automation, has transformed the sector, making it more vulnerable to cyber threats. This new reality presents significant challenges that require a coordinated and global response.

2.2 Cyberattacks against civil aviation are not just hypothetical threats—they are a tangible reality. Malicious actors can compromise critical systems such as air traffic control, navigation systems, and flight management systems, endangering the safety of millions of passengers and crew. Additionally, cyberattacks can cause severe operational disruptions, leading to significant economic losses and damaging the industry's reputation.

2.3 Main Cybersecurity Risks in Civil Aviation:

- Loss of Confidentiality: Theft of sensitive passenger and corporate data.
- Loss of Integrity: Manipulation of critical data affecting system functionality.
- Loss of Availability: Disruptions to air navigation services, communication systems, and other critical infrastructure.
- Reputational Damage: Loss of trust from passengers and stakeholders.

3. Conclusion

3.1 Given these challenges, it is imperative to adopt a comprehensive and collaborative approach to strengthen cybersecurity in civil aviation. As part of the strategic actions for implementing cybersecurity measures in the SAM Region, the following proposals should be considered:

3.1.1 Establishing a Solid Cybersecurity Framework for Civil Aviation: This framework would provide States and stakeholders with clear guidance on implementing effective security measures and should emphasize:

- Cybersecurity Policy: Minimum technical and regulatory cybersecurity guidelines for protecting critical IT/OT systems across all aviation stakeholders.
- Development of Specialized Talent: Investing in continuous cybersecurity training to build a highly skilled workforce, ensuring effective management of sensitive information and mitigating high turnover costs.

3.1.2 Develop guidelines to establish the organizational structure and operational procedures for a Civil Aviation Cybersecurity Incident Response Team (CSIRT), ensuring a faster and more coordinated

response to cyber incidents and minimizing their impact on air operations. This should include the following aspects:

- Centralization: Consolidate all incident response efforts into a single center, with the capacity to address all cyber events affecting critical aviation infrastructure and coordinate response actions.

- Coordination: Establish close collaboration with all relevant stakeholders within civil aviation in each Contracting State, as well as with other national and international CSIRTs, to facilitate information sharing and best practices.

- Training: Equip CSIRT personnel with the necessary tools and knowledge to effectively respond to cyber incidents affecting the aviation sector.

3.1.3 Collaboration among SAM Region States is essential for sharing information, best practices, and resources, as well as for developing a coordinated response to cross-border cyber threats. The following elements should be considered:

- Information Sharing: Develop a dedicated technological platform for cybersecurity information exchange within the civil aviation sector, enabling the sharing of experiences, knowledge, and lessons learned among all member States.

- Cooperation with SAM Region States: Strengthen cooperation between SAM Region States to jointly address cyber threats, including the development of joint simulation exercises and cyber incident management drills to assess risks to civil aviation.

- Create a cybersecurity training program tailored to the technical, operational, and executive personnel of the aviation sector. This program should cover all levels within aviation organizations, including:

- Operational Personnel: Raise awareness and provide training to air traffic controllers and other operational staff on cyber threat identification, security best practices, and incident response procedures.

- Technical Personnel: Offer specialized courses for Civil Aviation Security Inspectors and IT/OT personnel on system security, network protection, and cybersecurity controls for aviation technologies.

- Executive Leadership: Provide awareness programs and basic training in cybersecurity governance and policies specific to the aviation sector.

- Develop Human Capabilities: Cybersecurity training is crucial to ensuring that aviation personnel have the knowledge and skills necessary to prevent, detect, and respond to cyberattacks.

4. Suggested Action

4.1 The meeting is invited to:

a) Develop a Cybersecurity Framework or Action Plan that includes the elements outlined in this Study Note, serving as a reference for States and aviation sector stakeholders.

— END —