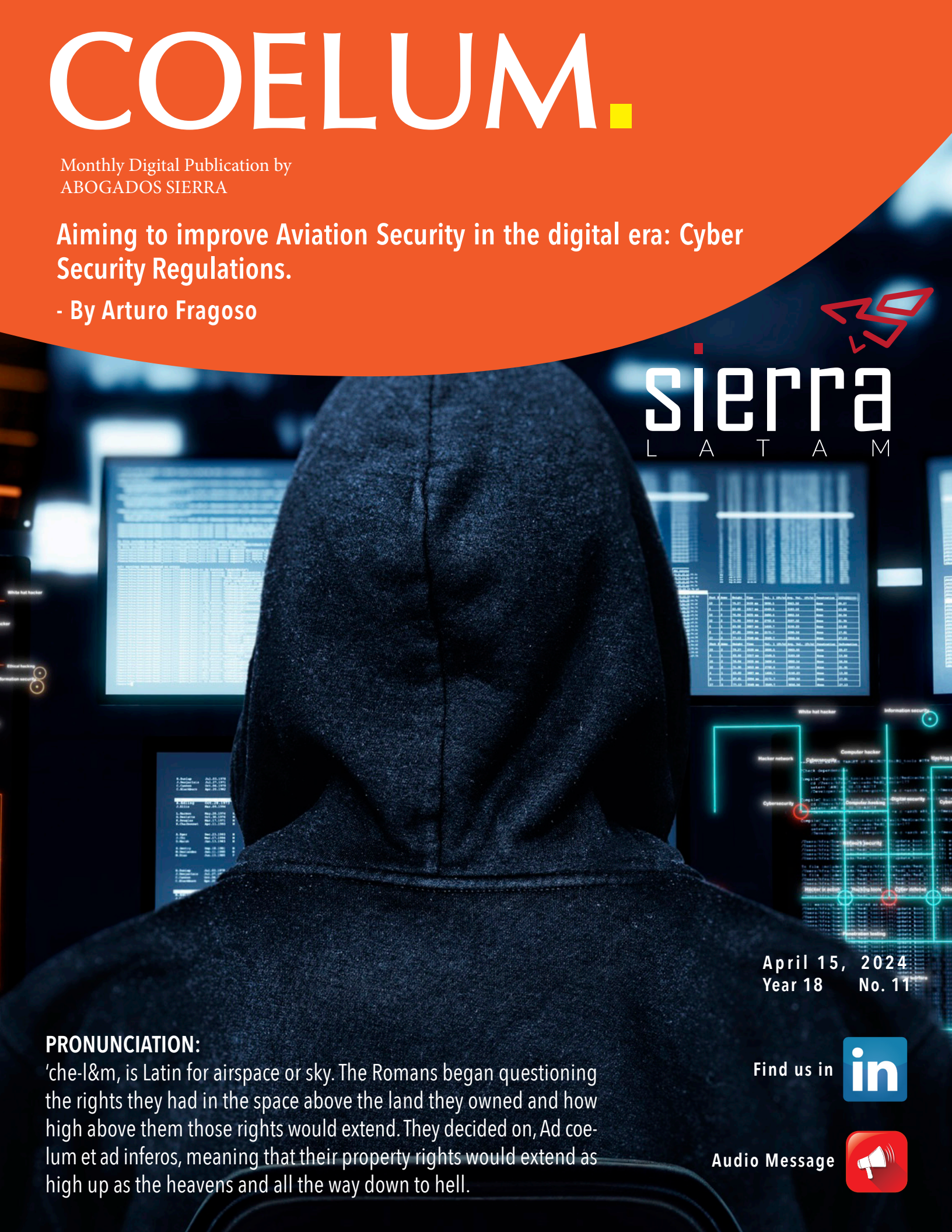
COELUM.

Monthly Digital Publication by
ABOGADOS SIERRA

Aiming to improve Aviation Security in the digital era: Cyber Security Regulations.

- By Arturo Fragoso

sierra LATAM



April 15, 2024
Year 18 No. 11

PRONUNCIATION:
'che-l&m, is Latin for airspace or sky. The Romans began questioning the rights they had in the space above the land they owned and how high above them those rights would extend. They decided on, Ad coelum et ad inferos, meaning that their property rights would extend as high up as the heavens and all the way down to hell.

Find us in

Audio Message

Aiming to improve Aviation Security in the digital era: Cyber Security Regulations.

Arturo Fragoso.

In an era marked by technological advancements and digital connectivity, ensuring the security of aviation systems has become paramount. Safety and security of international civil aviation have always been a priority within the industry. However, aviation security has taken on a new meaning with the rise of extremely violent terrorist activity against aviation. Upon Mexico's recovery of Category 1 status derived from the International Aviation Safety Assessment (IASA) Program, of the Federal Aviation Administration (FAA) from the U.S. Department of Transportation (DOT), the Federal Civil Aviation Agency (AFAC), Mexico's civil aviation regulatory authority, has continued to issue new regulations in alignment with the International Standards and Recommended Practices (SARPs), developed by the International Civil Aviation Organization (ICAO) in the Convention on International Civil Aviation (Chicago Convention).

These guidelines are intended to be applied universally to produce a high degree of technical uniformity and thus enable international civil aviation to develop safely and efficiently. Specifically, concerning the prevention and suppression of all acts of unlawful interference against civil aviation throughout the world, SARPs for international aviation security were first adopted by the ICAO Council in March 1974, and designated as Annex 17 to the Chicago Convention.

Enacted on February 09, 2024, Mandatory Circular number CO SA 17.18/24[1], a binding compliance technical resolution, was published on AFAC's official website to establish the minimum cyber security criteria that shall be met by air carriers and service providers to prevent acts of unlawful interference perpetrated through remote, cybernetic, computerized, or technological means of attack. In this regard, we will assess and undergo a comprehensive analysis throughout this paper to address the features of the recently developed new regulations concerning the industry needs and security aspects deemed essential to enhance and integral industry development in our country.

International Civil Aviation Framework

With the proliferation of digital technologies and interconnected systems in aviation, the need to address cybersecurity threats has become increasingly urgent. Annex 17 to the Convention on International Civil Aviation, titled 'Security: Safeguarding International Civil Aviation Against Acts of Unlawful Interference', serves as a cornerstone in addressing evolving threats to aviation security. While the primary focus of Annex 17 is on physical security measures to prevent unlawful interference with civil aviation, such as hijackings and sabotage, it also addresses emerging threats like cyber-attacks within its latest edition. Thus, Annex 17 acknowledges this reality and incorporates provisions specifically addressing cybersecurity to mitigate risks to aviation infrastructure, data, and operations. It provides guidance on protecting critical aviation infrastructure and systems from cyber threats, including requirements for risk assessments, security controls, and incident response procedures related to cybersecurity.

Within this context, cybersecurity measures aim to safeguard critical aviation systems and information against unauthorized access, manipulation, or disruption. Annex 17 mandates that States implement cybersecurity measures consistent with international standards and best practices to protect aviation infrastructure and

1.- Circular Obligatoria CO SA 17.18/24 que establece los requisitos mínimos de ciberseguridad que deberán implementar las personas concesionarias, asignatarias y permisionarias del transporte aéreo, aeródromos civiles, y prestadores de servicios aeroportuarios y complementarios para prevenir actos de interferencia ilícita perpetrados mediante medios de ataque remotos, cibernéticos, informáticos y tecnológicos, at https://www.gob.mx/cms/uploads/attachment/file/893544/co-sa-17-18-24-1r-19022024rev.pdf

data. It specifies requirements for conducting risk assessments, establishing security controls, and developing incident response plans tailored to cyber threats.

Therefore, SARPs within Annex 17 emphasize the importance of robust information security management systems in aviation organizations. These include measures to secure networks, systems, and data, as well as provisions for personnel training, access control, and encryption to mitigate cyber risks effectively. Annex 17 requires States and aviation stakeholders to establish procedures for reporting and responding to cybersecurity incidents promptly. This includes protocols for assessing the impact of incidents, sharing information with relevant authorities, and implementing corrective actions to prevent recurrence.

> ***"Within this context, cybersecurity measures aim to safeguard critical aviation systems and information against unauthorized access, manipulation, or disruption. Annex 17 mandates that States implement cybersecurity measures consistent with international standards and best practices to protect aviation infrastructure and data."***

Recognizing the transnational nature of cyber threats, Annex 17 encourages cooperation among States, international organizations, and industry stakeholders to enhance cybersecurity resilience in civil aviation. This includes information sharing, joint exercises, and capacity-building initiatives to address common challenges effectively. States are responsible for ensuring compliance with Annex 17 requirements within their jurisdictions and may adopt additional measures to strengthen cybersecurity in line with national laws and regulations. ICAO provides oversight and assistance to States in implementing cybersecurity SARPs and conducts audits to assess compliance levels.

Mexico's Regulations

For its part, Mexico, as a contracting state to the Chicago Convention, acknowledges its responsibility to supervise and regulate civil air transportation. This commitment is reflected in its latest amendment to the Civil Aviation Law, dated May 3, 2023. Through this amendment, Mexico has implemented several measures within its local legislation to uphold the safety of passengers, crews, ground personnel, and the general public in all aspects concerning protection against acts of unlawful interference.

These measures encompass the requirement for air transport operators and service providers to develop, implement, and regularly update a Security Program for the Prevention of Acts of Unlawful Interference. This program must be submitted to and approved by the Federal Civil Aviation Agency per the Civil Aviation Security Program of the Mexican State.

Of particular significance and under discussion is the new requirement placed on foreign carriers to establish, implement, and uphold civil aviation security procedures within national territory. These procedures are supplementary to the Security Program authorized by their respective Foreign Civil Aviation Authority. This requirement may be deemed contrary to the provisions outlined in Annex 9 of the Chicago Convention, 'Facilitation', which stipulates that such measures should aim to facilitate the mutual recognition of equivalent National Security Programs among contracting States.

Regarding the issuance of the referred Circular, the following obligations, including but not limited to, arose

from its publication, and came into force as of March 10, 2024:

- Compile an inventory of all information assets (software) and devices (hardware), identifying sensitive or critical data, information, and systems pertinent to regulation.
- Assess vulnerabilities across the Information Technology (IT) infrastructure and address them to minimize the window of opportunity for attacks.
- Implement processes and tools for tracking, controlling, preventing, and rectifying the use, allocation, and configuration of administrative privileges on computer equipment, networks, and applications.
- Establish, implement, and manage security configurations for mobile devices, laptops, servers, and workstations.
- Ensure protection for web browsers and emails to mitigate potential entry and attack points.
- Exercise control over the installation, propagation, and execution of malicious code across various organizational points.
- Implement processes and tools for monitoring, controlling, preventing, and rectifying the secure utilization of wireless networks (WLAN), access points, and wireless client systems.
- Institute cybersecurity awareness and training programs to evaluate, identify gaps, and remediate through policy reinforcement, organizational planning, and targeted training initiatives.
- Conduct semi-annual penetration tests or "red teaming" exercises across IT infrastructure to assess resilience and identify areas for improvement.

In terms of compliance, the regulatory entity is obligated to prepare and submit a semi-annual report outlining the measures implemented. This report should include, firstly, an account of any attacks or attempted illicit interferences, detailing their characteristics. Additionally, the entity must provide a report on the penetration test or network red teaming exercise conducted by an Authorized Verification Unit[2].

Conclusions

With millions of passengers and cargo tonnage flown every year, the aviation industry is a high-profile target for terrorists and hostile acts around the world. The enactment of cybersecurity provisions reflects a proactive approach to address emerging threats in an increasingly digital environment. However, challenges remain in effectively implementing and enforcing cybersecurity measures across diverse operational contexts. To enhance aviation security in the digital age, policymakers, regulators, and industry stakeholders must prioritise collaboration, innovation, and capacity building. This includes investing in cybersecurity infrastructure, fostering information-sharing mechanisms, and promoting a culture of cybersecurity awareness and resilience throughout the aviation sector.

Whilst Annex 17 and its related SARPs represent a critical step forward in safeguarding international civil aviation, national legislation must ensure due and efficient implementation of guidelines, not solely by incorporating cybersecurity principles into aviation security policies and provisions but by mitigating risks, enhancing resilience, and promoting secure and sustainable air transport operations. Continued vigilance, cooperation, and adaptation are essential to address evolving cyber threats effectively and maintain the integrity and safety of the aviation industry. Undoubtedly, all relevant stakeholders should be working on enhancing civil aviation, mostly in terms of security and safety, however, the mutual recognition of National Security Programs of contracting States shall be also part of the discussion.

.

2.- Units authorized by the AFAC, responsible for monitoring compliance with the provisions of the Circular. They are required to possess a minimum of three years' experience in auditing computer systems and managing information security, ensure their personnel have no criminal records, have entered into a collaboration agreement with the AFAC, and demonstrate possession of at least one of the following certifications: Certified Ethical Hacker (CEH), Certified Ethical Hacker and Security Professional (CEHSP), Offensive Security Certified Professional (OSCP), Certified Penetration Testing Specialist (CPTS), o NIST Cybersecurity Framework Lead Implementer.

COELUM.

ARTURO FRAGOSO
Associate

Arturo is an associate in the Regulatory area. With over 5 years of experience advising on regulatory and compliance aspects of aviation law, he specializes in representing the interests of international air carriers in Mexico. He liaises with relevant regulatory and airport entities in Mexico to ensure safe operations and provide top-tier legal services to reputable air carriers and related companies. In addition to his focus on aviation law, Arturo offers comprehensive legal guidance to Mexican and foreign entities across various aspects of corporate law. This includes assisting with the necessary steps for conducting business in Mexico and ensuring compliance with all corporate and tax requirements. His practice encompasses aviation industry matters, airport law, labour law, and corporate law, all geared towards providing clients with precise, effective legal solutionsc.

Education:
- Attorney at law by Instituto Tecnológico de Estudios Superiores de Monterrey in Mexico City.
- Undergraduate studies abroad in International Public Law and Commercial Law in Monash University, in Melbourne, Australia.

Memberships:
- Member of the Mexican Contact Group for the Aviation Working Group

Publications:
Arturo has authored numerous articles focusing on the regulatory aspects of aircraft and airline operations, as well as other pertinent topics concerning Mexico's legislation, in COELUM and TERRUM.

Languages:
- English
- Spanish

sierra
LATAM

Prol. Reforma No. 1190 25th Floor,
Santa Fe México D.F. 05349
t. (52.55) 52.92.78.14
www.asyv.com / www.asyv.aero

www.linkedin.com/company/asyv