International Civil Aviation Organization
South American Regional Office
Seventeenth Meeting of Civil Aviation Authorities of the SAM Region (RAAC/17)
(Santiago, Chile, 10 to 14 April 2023)

Agenda Item 1A: Current situation and regional priorities

ASSESSMENT OF TECHNICAL DOCUMENT ON CIVIL AVIATION CYBERSECURITY

(Presented by Chile)

SUMMARY

The purpose of this paper is to submit to RAAC/17 a proposal for a technical document containing the general cybersecurity fundamentals on the basis of which networks and systems used for the provision of regulated aeronautical services must be designed, installed and operated in a secure manner, to serve as a guide for SAM States to establish a regulatory framework on this matter.

References:

- Aviation cybersecurity strategy
- Cybersecurity Action Plan
- ISO 27001:2022
- ISO 27002:2022
- ISO 27035-1:2016

ICAO strategic objective:	*Security and facilitation*

1. Background

1.1 The current trend in national and international aviation system management is rapidly moving towards change and integration as a result of digital transformation and the increased need for greater information sharing, creating a common awareness with a broad spectrum of aviation stakeholders that can certainly improve operational efficiency and increase productivity, but this is also where the potential for a cyberattack opens up.

1.2 Vulnerabilities are growing because current and next generation systems require more information exchange using commercially available technology, such as shared networks and computing infrastructures, network-centric architectures and operations, and unlike the past, information exchange in the future will not be limited to point-to-point communications, but will also use open systems architecture and internet-based information flow. Furthermore, the control systems of the different areas of operation have moved towards greater use of existing technologies, increasing interoperability between systems and the use of automation to improve productivity, where the identification of threats is key to risk management for each threat. Aeronautical fixed services (AFS) establish a series of identified threats, such as: information flooding, passive interception of information, active interception of information, modification of system configuration or data, destruction of system configuration, disruption or denial of service attacks.

2. **Discussion**

2.1 States are invited to discuss the creation of a technical document to serve as a basis for including in national civil aviation security programmes (NCASPs) and other relevant national programmes appropriate provisions to protect the aforementioned critical systems, including their hardware and software, against cyberattacks and interference.

3. **Suggested action**

3.1 The Meeting is invited to:

a) take note of this paper and its Appendix A; and
b) review and discuss the proposal presented in Appendix A.

- - - - -

APPENDIX A

TECHNICAL DOCUMENT ON AVIATION CYBERSECURITY

Title I. General

1. Purpose

The purpose of this technical document is to establish a regulatory framework comprising the general cybersecurity fundamentals on the basis of which networks and systems used for the provision of regulated aeronautical services must be designed, installed and operated in a secure manner, for the protection and resilience of networks, systems and their operational continuity, confidentiality, integrity and availability of information.

This standard covers cybersecurity risk management aspects in the area of aeronautical services regulated by law, including the operational impact analysis, risks and mitigation measures. It also identifies the life cycle of a cyber-incident, and the corresponding prevention, detection, analysis, notification, containment, eradication, recovery and documentation.

It also seeks to establish guidelines for the reporting of cyber-events by operators and aeronautical service companies to the responsible authority, either directly or through the entity designated by the latter, in order to coordinate actions aimed at mitigating their effects and impacts and contribute to the timely normalisation and stabilisation of the affected services.

2. Definitions

For the purposes of this technical standard, the following terms shall have the meaning described below:

- ✓ Authentication:

Process used in access control mechanisms to verify the identity of a user, device or system by checking access credentials.

- ✓ Cyberspace:

The global and dynamic domain within the information environment that corresponds to the setting composed of technological infrastructure, logical components of information, data (stored, processed or transmitted) covering the physical, virtual and cognitive domains, and the social interactions that take place therein.

Technological infrastructure means the physical equipment used for the transmission of communications, such as links, routers, switches, stations, radiating systems, nodes, conductors, among others. The logical components of information are the different software that enable the operation, management and use of the network.

- ✓ Cyber-incidence or cyber-incident:

Any event that compromises the availability, authenticity, integrity or confidentiality of systems or stored, transmitted or processed computer data, or the corresponding services offered by the information systems and their infrastructure, which may affect their normal operation.

- ✓ Cyber-security:

Set of possible actions for the prevention, mitigation, investigation and management of threats and incidents on information assets, data and services, as well as for the reduction of their effects and the damage caused before, during and after their occurrence.

- ✓ Cyber-attack:

Any deliberately provoked cyber-incident affecting a computer system.

- ✓ Confidentiality:

Security principle requiring that data be only accessed by authorised personnel.

- ✓ Availability:

Ability to be accessible and ready for use on demand by an authorised entity.

- ✓ Integrity:

Security principle that certifies that data and settings are only modified by authorised personnel and activities. Integrity considers all possible causes of modification, including software and hardware failures, environmental events and human intervention.

- ✓ Cybersecurity incident response coordination centre

Centres staffed by specialists trained to coordinate the response to cybersecurity incidents in a quick and effective manner.

- ✓ Incident management:

Procedures for the detection, analysis, handling, containment, containment and resolution of a cybersecurity incident, and responding to it.

- ✓ Incident:

Unexpected or undesired event with consequences detrimental to the security of aeronautical information networks and systems.

- ✓ Critical aeronautical Information infrastructure

Physical and information technology facilities, networks, services, and equipment whose disruption, degradation, denial, interruption, or destruction may have a significant impact on safety or the economic well-being of citizens or the effective functioning of the State.

- ✓ Technological neutrality:

Regulatory principle whereby the technical rules aimed at limiting the negative externalities of an activity must describe the outcome to be obtained but giving the regulated parties the freedom to adopt the most appropriate technology to achieve the outcome. It also implies applying the same regulatory principles regardless of the technology used, and that the regulation is not used as a means to drive the market towards a particular structure that the regulator considers optimal.

- ✓ Non-repudiation:

A security service that provides the sender and receiver of data with proof of the origin and destination of the data, which can be used in the event of attempts by the sender or receiver to deny its transmission.

- ✓ Resilience:

Ability of systems or networks to continue to operate despite being subjected to an incident or cyber-attack, even if in a degraded, weakened, or segmented state. It also includes the ability to promptly restore essential functions after an incident or attack, so as to recover promptly from a disruption, usually with minimal recognisable effect.

- ✓ Risk:

Any reasonably identifiable circumstance or fact that has a potential adverse effect on the security of telecommunications networks and information systems. It can be quantified as the probability of materialisation of a threat that produces an impact in terms of operability, physical integrity of individuals or material or corporate image.

Any other term not defined in this technical standard will have the meaning attributed to it in the respective aeronautical sector regulations.

3. Scope of application

This standard has a scope of application in:

- ✓ Air terminal operators
- ✓ Air cargo terminal operators
- ✓ Aircraft operators
- ✓ Service companies, operating in aerodromes and airports
- ✓ Aeronautical service providers

4. Statement of relevance

The civil aviation operational environment is changing rapidly and significantly with the introduction of new advanced technologies and communication systems that migrate from manual procedures to more effective automated procedures, communications, and archiving, with a view to enhancing security and facilitation.

Aeronautical operators, including aircraft and airport operators, air traffic service providers and others, should identify the software and hardware used for critical information systems in their operations, which may include, but are not limited to, the following systems used for:

- access control and alarm monitoring;
- departure control;
- baggage matching with passengers;
- inspection or detection of explosives, by means of networked or stand-alone systems;
- databases on regulated agents and known shippers;
- air traffic management;
- operator bookings and passenger check-in;
- closed-circuit television surveillance; and
- security command, control, and dispatch.

Potential vulnerabilities in the use of such systems include the increased number of connections or links between ground systems and aircraft, as well as the use of commercially purchased software and hardware. The safety of passengers, crew and ground personnel would be put at risk in case of interference with such systems. Likewise, personal information on passengers and employees should be protected against unauthorised access and use.

Article 5. General cybersecurity obligations

The objective of this industry standard is to include in the national civil aviation security programmes (NCASP) and other relevant national programmes appropriate provisions to protect the aforementioned critical systems, including their hardware and software, against cyberattacks and interference.

A. Protection of critical information systems

Physical protection of the CAA's critical information systems should start at the design stage, or as early as possible, to ensure that they are as resilient as possible to cyber-attacks. This can be achieved by applying a multi-layered approach, which involves, inter alia:

- administrtive controls, such as:
  - ✓ security standards, policies and procedures;
  - ✓ appropriate recruitment, selection and training of personnel, particularly those with rights as administrators, including background checks;
  - ✓ threat and risk assessment to determine the vulnerability of a system and the likelihood of an attack;
  - ✓ quality control, including inspections and tests; and
  - ✓ hardware and software supply chain security.

- virtual or logical controls, such as:
  - ✓ firewalls;
  - ✓ data encryption;
  - ✓ network intrusion detection system; and
  - ✓ anti-virus systems.

- physical controls, such as:
  - ✓ ensure that system hardware, particularly servers, is properly protected and located in access-controlled areas;
  - ✓ implement authentication systems, such as biometric registration methods or passwords, that limit access to the system to authorised persons only;
  - ✓ limit the number of persons with authorised access;
  - ✓ require more than one person for approvals within the systems, *e.g.* produce airport identification permits only if authorised by two persons;
  - ✓ monitor and control access to systems on an ongoing basis;
  - ✓ use remote contingency systems in case of failure of the main system; and
  - ✓ maintain activity logs that can be used for audits and assessments and provide alerts in case of activities outside normal operational parameters.

The protection of critical aeronautical information and communitation technology (ICT) systems, including their hardware, software and data, should be included in the established threat assessment procedures.

The DGCA will require operators to assess the vulnerability of their aeronautical ICT systems, establish measures to address potential cyber-attacks and verify the implementation of such measures as part of their regular compliance oversight activities such as inspections and audits.

B. Infrastructure security measures

- Security through design
  - ✓ The CAA will ensure that operators include security measures in the design, implementation and operation of new aeronautical information technology and communications systems, including the disposal of hardware and software. To the extent possible, these measures must be applied to modifications to existing systems.

Thus, if implemented at an early stage, the design and construction of airport and aircraft operator facilities, such as check-in and boarding counters or ticket counters, check points and cargo and logistics centres for airport supplies, will be more appropriate.

- ✓ Security provisions should be included in the specifications for new aeronautical ICT systems and their procurement. Providers must supply information on how the information and operation of the system is protected, including arrangements for ongoing support and maintenance, whether on-site or remote. Preventive maintenance must be scheduled and managed; if support and maintenance are outsourced, the number of people allowed access to system hardware and software should be limited. Also, cable pathways must be designed so that critical aeronautical information systems cannot be easily infiltrated.

- Separation between networks
  - ✓ The DGCA shall ensure that networks used for critical aeronautical ICT systems are separated from publicly accessible networks.
  - ✓ The software and hardware of a modern aeronautical communication and information system cannot function without the necessary cabling and connection to another network of operational systems to facilitate data transmission and exchange. For this reason, systems must be examined to ensure that security objectives are not compromised by exposure to uncontrolled or open-access communication networks. Likewise, appropriate policies and practices must be established to minimise the connections required. This practice is often referred to as "hardening".
  - ✓ Connections to networks must be made under controlled conditions where the type of information and the frequency or method of data exchange between the system and the network are known. An effective management system for such interfaces must be established to ensure that all connections to a system are documented, reviewed and updated as appropriate, and that adequate protection against viruses and malware is in place if necessary.
  - ✓ A multi-layered approach to software management must be considered. A limited number of individuals must have rights as administrators of a critical aeronautical ICT system. Access to the system should be based on the principle of legitimate need. Thus, some individuals could be granted only read-only rights, while others could be authorised to have access only to those parts of the system that relate to their specific tasks.

- Remote access
  - ✓ It shall be ensured that remote access to critical aeronautical ICT systems is only permitted under pre-established and secure conditions, and that suppliers do not have unauthorised access once such systems have been procured or installed.
  - ✓ In most cases, remote system access will require suppliers to have an appropriate means of remote access. Operators must ensure that they are aware of the means of such access and that they are aware of input method and conditions.
  - ✓ Only authorised personnel must carry out systems maintenance on pre-arranged and approved days and times. Operators should require suppliers to limit the number of persons authorised to provide system support and maintenance. Such persons should be subject to background checks, including criminal records to the extent permitted by law.
  - ✓ The DGCA may add to the above measures an appropriate audit and an exemption reporting system that generates an automatic report whenever abnormal activity

occurs in the system, such as access outside normal working hours. Audit logs will be regularly reviewed to identify exceptional access and examine its circumstances.

- ✓ The DGCA and operators should request a certificate from suppliers stating that there is no backdoor access and guaranteeing the integrity of the system. This would be useful in the event of the need for prosecution.

C. Supply chain security for hardware and software

- Aeronautical ICT systems need to be periodically upgraded due to changes in operational requirements or software upgrades and often require software or hardware to be modified.
- Measures must be in place to ensure that only recognised and legitimate suppliers are used to procure software and hardware for aeronautical ICT systems. To the extent possible, the supply chain security concept must be applied. The objective of this measure is to ensure that the integrity of software and hardware is protected against unauthorised interference throughout the supply chain. Suppliers must be required to report on their own security measures not only at the installation stage, but also throughout the useful life of the system.

D. Records of cyber-attack incidents

Understanding the threat and potential attack methods is an essential element in developing appropriate security measures to protect aeronautical ICT systems against cyber-attacks. A number of measures must be taken for this to be effective, including, but not limited to, the following:

- develop and implement a template for reporting cyber-attack incidents. This will facilitate the collection and analysis of information, including threat assessment, and the implementation of appropriate countermeasures;
- establish an alert system to facilitate communication with operators and other stakeholders; and
- establish provisions to require operators to implement a reporting regime in their organisations and include it in their security programmes.

E. Cybersecurity considerations in airport operations

- Departure control system
  - ✓ Providers shall ensure redundancy, backup systems or contingency protocols in the event of failure of the departure control system.
  - ✓ Providers must have standard means to mitigate denial of service attacks and protect their networks from intrusion.

- Flight information display system
  - ✓ Unauthorised agents must be prevented from physically accessing the flight information display systems.
  - ✓ Physical security backups, announcements or deployment of personnel to direct passengers must be considered in the event of failure of this system.

- Airport operational database
  - ✓ Security of access control to the operational database must be ensured and human intervention will only be required when there is a malfunction of the database.

- Baggage handling system
  - ✓ These systems installed in different terminals should be segregated / separated.
  - ✓ Consideration should be given to the possibility of using some elements in isolation from the overall system to partially restore service in case of contingency (*e.g.* manual operation of conveyor belts without full automation / baggage handling).

- Main area search scanner
  - ✓ Physical, software and network security controls of the scanning equipment must be ensured.
  - ✓ If machines are managed remotely, the degree of connectivity must be isolated from other networks and monitored on an ongoing basis.
  - ✓ Detection systems must be implemented in case of major and widespread equipment failures.
  - ✓ Logical or physical separation of business/operational infrastructure in higher risk environments must be ensured.
  - ✓ Personnel verification procedures and security practices must be implemented to protect access to equipment.
  - ✓ A procedure for updating the database for this equipment must be established.

- Physical access control system
  - ✓ Procedures must be implemented for screening all personnel with access to the area of operations and security controls on access to restricted areas.
  - ✓ Procedures for security patrols and control of the physical perimeter must be implemented on an ongoing basis.

- Building integration system
  - ✓ For the integration of the different buildings within an airport, robust network defences, perimeter protection, intrusion detection, etc. must be implemented.

- Surface movement radar
  - ✓ Physical security controls must be implemented to prevent disruption of aircraft operations.

- Lighting control and monitoring system
  - ✓ Physical security controls must be implemented to prevent aircraft operations from being seriously affected at certain times of the day.

5. Cyber-incident reporting obligations

A. **Classification of incidents**

	Class	Type	Description
1	Abusive content	Child pornography– Sexual – Violence	Child pornography, violence glorification, other.
		Spam	"Unsolicited bulk mail, which means that the recipient has not given verifiable permission for the message to be sent and, besides, the message is sent as part of a bulk group of messages, all having similar content.
		Defamation	Discrediting or discriminating against someone.

	Class	Type	Description
2	Malicious code	Malware, Virus, Worms, Trojans, spyware, Dialer, rootkit	Software that is intentionally included or inserted into a system for a harmful purpose. Usually requires user interaction to activate the code.
3	Information collection	Scanning	Attacks that send requests to a system to discover weaknesses. Some form of testing process is also included to gather information about hosts, services and accounts. Examples: fingerd, DNS queries, ICMP, SMTP (EXPN, RCPT, ...), port scanning.
		Sniffing	Observing and recording network traffic (telephone or data network tapping).
		Social engineering	Collecting information from a human being in a non-technical way (*e.g.* lies, tricks, bribes or threats).
4	Intrusion attempts	Access attempts	Multiple login attempts (guessing / cracking passwords, brute force).
		Exploitation of known vulnerabilities	An attempt to compromise a system or disrupt any service by exploiting known vulnerabilities that already have their standard CVE identifier (*e.g.* buffer overflow, backdoor, cross scripting, etc.).
		New attack signature	An attempt to use an unknown exploit.
5	Intrusion	Privileged account compromise	A successful compromise of a system or application (service). This may have been caused remotely by a known or new vulnerability, but also by unauthorised local access. It also includes being part of a botnet.
		Unprivileged account compromise	
		Application compromise, bot	
6	Availability	Denial of service (DoS / DDoS) attack	With this type of attack, a system is bombarded with so many packets that operations are delayed, or the system fails. Examples of DoS are ICMP and SYN floods, teardrop attacks and mail bombardment. DDoS is often based on DoS attacks originating from botnets, but there are also other scenarios such as DNS amplification attacks. However, availability can also be affected by local actions (destruction, power supply interruption, etc.), spontaneous failures or human error, without malicious intent or negligence.
		Sabotage	
		Interception of information	
7	Content security information	Unauthorised access to information	In addition to local abuse of data and systems, information security can be jeopardised by a successful account or application compromise. Furthermore, attacks that intercept and access information during transmission (telephone tapping, spoofing or hijacking) are possible. Human / configuration / software error can also be the cause.
		Unauthorised modification of information	
8	Fraud	Phishing	Disguised as another entity to persuade the user to reveal a private credential.
		Copyright	Offering or installing copies of unlicensed commercial software or other copyrighted materials (Warez).
		Unauthorised use of resources	Using resources for unauthorised purposes, including corporate benefits (*e.g.* use of email to engage in illegal profit chain letters or pyramid schemes).
		Forging of records or identity	Type of attacks in which one entity illegally assumes the identity of another in order to profit from it.
9	Vulnerable	Open systems and/or software	Open resolver systems, printers open to everyone, apparent vulnerabilities detected with nessus or other applications, virus signatures not updated, etc.

	Class	Type	Description
10	Others	All incidents that do not fit into any of the above categories	If the number of incidents in this category increases, it is an indicator that the classification scheme must be revised.
11	Test	For testing	Product of controlled and reported security testing.

B. Level of danger

The level of danger determines the potential threat that the occurrence of an incident would pose to the operator's networks and systems, as well as to the quality or continuity of the services provided. This indicator is based on the intrinsic characteristics of the type of threat.

According to their characteristics, threats will be classified with the following hazard levels: Critical, Very High, High, Medium and Low. The level assigned will be determined as indicated in the table below:

Figure 2. Levels of danger of cyber-incidents

CRITERIA FOR DETERMINING THE LEVEL OF HAZARD		
Level	Classsification	**Type of Incident**
CRITICAL	Others	**APT**
VERY HIGH	Malicious code	**Malware distribution**
		Malware configuration
	Intrusion	**Theft**
	Availability	**Sabotage**
		Interruptions
HIGH	Abusive content	**Child pornography, inappropriate sexual or violent content**
	Malicious code	**Infected system**
		Command and control (C&C) server
	Intrusion	**Application compromise**
		Privileged account compromise
	Intrusion attempt	**Unknown attack**
	Availability	**Denial of service (DoS)**
		Distributed denial of service (DDoS)

Level	Classsification	Type of Incident
	Information compromise	**Unauthorised access to information**
		Unauthorised modification of information
		Loss of data
	Fraud	**Phishing**
MEDIUM	Abusive content	Hate speech
	Acquisition of information	Social engineering
	Intrusion attempt	Exploitation of known vulnerabilities
		Attempted access with credential breach
	Intrusion	Compromise of unprivileged accounts
	Availability	Misconfiguration
	Fraud	Unauthorised use of resources
		Copyright
		Impersonation
	Vulnerable	Weak cryptography
		DDoS amplifier
		Services with potential unwanted access
		Information disclosure
		Vulnerable system
LOW	Abusive content	Spam
	Acquisition of information	Network scanning
		Packet analysis (sniffing)

A. Level of impact

The criteria used to determine the level of impact associated with a cyber-incident are based on the following parameters, with no predetermined order of priority or importance:

- ✓ Impact on national or public security.
- ✓ Effects on the provision of a telecommunication service or on a critical infrastructure.
- ✓ Type of information or systems affected.
- ✓ Degree to which the organisation's facilities are affected.
- ✓ Possible interruption in the provision of the organisation's normal service.
- ✓ Time and own and external costs until the recovery of the normal operation of the facilities.
- ✓ Economic losses.
- ✓ Geographical extent affected.
- ✓ Associated reputational damage.

The possible levels of impact of a cyber-incident are Critical, Very High, High, Medium, Low or No Impact. The corresponding level of impact will be assigned using the following table as a reference:

CYBER-INCIDENCE LEVEL OF IMPACT	
Level	**Description**
CRITICAL	Significantly affects national security.
	Affects public safety, with potential danger to people's lives.
	Affects a critical infrastructure.
	Affects systems classified as SECRET
	Affects more than 90% of the organisation's systems.
	Interruption in the provision of service for more than 24 hours and more than 50% of users.
	The cyber-incident requires more than 100 person-days to resolve.
	Economic impact of more than 0.1% of the current GDP.
	Supranational geographical extent.
	Very high reputational damage and continuous coverage in the international media.
VERY HIGH	Affects public security with potential danger to property.
	Significantly affects official activities or missions abroad.
	Affects an essential service.
	Affects systems classified as RESTRICTED.
	Affects more than 75% of the organisation's systems.
	Interruption in the provision of the service for more than 8 hours and more than 35% of users.
	The cyber-incident requires between 30 and 100 person-days to resolve.
	Economic impact between 0.07% and 0.1% of the current GDP.
	Geographical extent of more than 4 CC. AA. or 1 T.I.S.
	Reputational damage to the country's image.
	High reputational damage and continuous coverage in national media.
HIGH	Affects more than 50% of the organisation's systems.
	Interruption in service provision for more than 1 hour and more than 10% of users.

CYBER-INCIDENCE LEVEL OF IMPACT	
Level	**Description**
	The cyber-incident requires between 5 and 30 person-days to resolve.

6. Article 8. Contents of the reports

Parties bound by this standard shall report in a timely and proper manner all the information relating to the cyber-incidence that is required. However, in the initial report, they shall only provide the information they are aware of at that time and should complete it in subsequent reports.

Cyber-incident reports should contain at least the following information fields:

- ✓ Executive summary of the cyber-incident.
- ✓ Identification of the relevant operator.
- ✓ Acting cyber-security officer.
- ✓ Precise date and time of occurrence of the cyber-incident.
- ✓ Precise date and time of detection of the cyber-incident.
- ✓ Detailed description of the event.
- ✓ Technological resources affected.
- ✓ Identifiable origin or cause of the cyber-incident.
- ✓ Taxonomy, classification, or type of cyber-incident.
- ✓ Level of danger.
- ✓ Impact level.
- ✓ Cross-border impact, if applicable.
- ✓ Compromise indicators: IP level compromise indicators, domain and subdomain level compromise indicators, mail compromise indicators, MD5 level compromise indicators, among others.
- ✓ Action plan and resolution and mitigation measures.
- ✓ Current and potential affected parties.
- ✓ Means required for resolution calculated in man/person-hours (HH).
- ✓ Estimated economic impact, if applicable and known.
- ✓ Geographical extent, if known.
- ✓ Reputational damage, even if potential.
- ✓ Logs automatically generated by the systems.
- ✓ Background information attached, if applicable.

In the particular case of cyber-incidents that affect or may affect critical infrastructure, the report shall indicate the reasons why a report does not contain all relevant information, which shall be sent as soon as it is obtained.

For cyber-incidents affecting critical infrastructure or impacting strategic sectors, the operator shall contract an independent forensic analysis, indicating the measures taken for their proper mitigation and resolution.

7. Article 9. Timing of reports

Operators affected by a cyber-incident shall generate a mandatory report, which shall be submitted in a timely and proper manner, to include an initial report, intermediate reports and a final report.

The initial report is a communication to raise awareness and alert of the existence of a cyber-incident.

Intermediate reports provide updated data available at that time in relation to the reported cyber-incident. As many intermediate reports as deemed necessary will be made from the time the initial immediate report was generated.

The final report expands and confirms the final data in relation to the reported cyber-incident as of the day on which the initial immediate report was generated.

Whenever possible, the report will be submitted in writing using the means indicated by the DGCA for this purpose or, if not available, by e-mail or, failing that, by the most suitable means available.

Timing of mandatory reports			
Level of Danger	**Initial Report**	**Intermediate Report**	**Final Report**
Critical	Immediate	3/ 6/ 12/ 24/ 48 hours	Maximum 10 days
Very high	Immediate	48 / 72 hours	Maximum 20 days
High	Immediate	No deadline	Maximum 30 days

Reports shall be sent in a timely and successive manner as the cyber-incident unfolds, incorporating all relevant information and reporting each material change as it occurs. Likewise, the operator shall implement security measures during the process of transmitting incident reports.

A record should be kept of the evolution of the cyber-incident as it develops and, where critical infrastructure may be affected or is affected, the record should be extended until it has been closed, *i.e.* fully resolved.

8. Treatment of the reports

Cyber-incident reports will be treated as confidential documentation by the State entities that become aware of them, especially the data that could expose the operator's own technical background information, that puts the operator's cyber-security at risk, as well as customer information in accordance with privacy legislation.

9. Information to third parties and exchange of information

In case of reporting and/or alerting third parties to prevent, manage or resolve a cyber-incident, the relevant operator may request the assistance of the Computer Security Incident Response Team (CSIRT) or other body designated by the competent authority for such purposes, if appropriate. In the event of requiring support from response teams abroad, the operator shall ensure the privacy and due protection of the data involved.

In turn, the DGCA, the incident response coordination centre, or the body designated by the DGCA for such purposes, will act in accordance with the indications contained in the reports regarding the impact that the dissemination of the information contained therein may have in accordance with the Traffic Light Protocol (TLP). If it is deemed necessary to disseminate the information to third parties beyond the scope of the TLP designation indicated by the author of the report, authorisation from the original source will be required. In general, any data that could expose the operator's own technical background information, which could put the operator's cyber-security at risk, as well as any information on its users, will not be disclosed, in accordance with the provisions of the law on privacy protection.

If it is decided to directly inform the public or third parties, the publication will be aimed at providing information on the cyber-incidents, possible causes, mitigation measures, security recommendations, alternative actions to be taken, geographical areas or systems affected and any other information of importance for the correct and timely information of the general public, without affecting the reputation of those involved.

Likewise, in accordance with the powers conferred by the applicable legislation, the DGCA will take measures and steps to promote the exchange of information on matters of security and cyber-security of networks and information systems between public and private actors, in order to adopt the relevant measures in these matters.

Title VI, Resolution of cyber-incidents

10. Obligation to resolve cyber-incidents

Once a cyber-incident affecting a network or system used for the provision of aeronautical services has been detected, the respective operator shall take all necessary steps in a timely manner to resolve it and restore the normal provision of the affected services, in accordance with its risk management plan and, in all cases, giving first priority to those measures that prevent or, failing that, minimise the impact on end users.

In the event that the operator concerned deems it necessary for the resolution of a cyber-incident, it may request cooperation from the DGCA or other entities competent in cyber-security matters, such as the reference CSIRT designated by the DGCA or other computer incident response teams.

Operators shall provide additional information as required to analyse the nature, causes and effects of the reported incidents, as well as to compile statistics and gather the necessary data for performance reporting. The additional information provided will be treated with confidentiality and will not be used for any purpose other than those authorised.

Furthermore, without detriment to immediate measures leading to the mitigation of the effects and the restoration of services affected by a cyber-incident, operators shall, to the extent technically feasible, according to substantiated supporting information, remedy vulnerabilities in their systems that have enabled or facilitated cyber-incidents.

If an operator detects that its networks and systems have been used as a means of committing cybercrime, the operator shall file complaints with the competent bodies, take appropriate legal action and inform the DGCA.

Each operator will be liable, after due process in accordance with the Constitution and laws, for any loss or leakage of information resulting from its negligence with respect to the receipt, holding, handling, storage, and delivery of information transmitted or deposited in custody in the provider's systems, in order to ensure the certainty, confidentiality, security and non-repudiation of the communication.

The operator must establish protocols for the recovery of information in the event of loss of information due to tampering, cyber-incidents, or other causes for which the operator is responsible.

11. Safeguarding of personal and sensitive data

Any personal data or information of a sensitive nature, as well as any other information from which it could be inferred, shall be omitted from cyber-incident reports. Likewise, in cases where the competent authority instructs the operator to send a copy of a report to a third party, all personal data, or data from which the identity of the person concerned can be inferred shall be removed.

In the event that the analysis of a cyber-incident reveals the occurrence of a possible personal data breach, the body designated for this purpose shall forward the relevant reports to the competent data protection authority. Together with the relevant sections of the reports, the reasons why there may have been a breach of personal data pursuant to Law No. 19.628 will be indicated.

In all cases, consideration shall be given to the regulations on the use of user information and metadata, whether for the operator's own benefit or that of third parties, without the express authorisation of the client, in accordance with the provisions of Article 9 of the aforementioned Law Nº 19.628 on the Protection of Privacy, and in accordance with the cross-cutting principles of human rights recognised by the international community.

Title VII, Mandatory reporting of modification to networks and systems

12. Periodic reports

Relevant operators shall send to the DGCA, either directly or through the body designated by the DGCA for this purpose, periodic reports on the modifications introduced in their networks and systems, either in the software layer or in hardware elements, to address the vulnerabilities detected in the last reported period. The reporting period will be every three months.

The aforementioned reporting requirements will be mandatory on a six-monthly basis for non-relevant operators.

The DGCA will use the information provided in the periodic reports only for statistical purposes and in studies for policy-making.

Title VIII, Non-mandatory reports

13. Non-mandatory reports

Providers that are not considered relevant operators may submit cyber-incident reports to the DGCA, the reference CSIRT or the body designated for such purposes. Likewise, any telecommunication service provider may report cyber-incidents that do not meet the mandatory reporting thresholds specified in Article 7. In any case, any report of a cyber-incident will oblige the respective operator to continue reporting the development of the incident, if applicable under this technical document, and to manage its resolution.

In turn, the competent authorities may assess in a different way the priorities with which non-mandatory reports are handled in relation to mandatory reports.

Title IX, Security monitoring

14. Security monitoring

Relevant operators shall maintain continuously updated risk management plans for the telecommunication networks and systems they use for the provision of authorised services. Such plans shall be formulated in such a way as to anticipate consequences arising from threats such as cyber-attacks and non-hostile cyber-incidents, based on an analysis and assessment of the risks to which their networks and systems are exposed, with the objective of avoiding or reducing the occurrence of such contingencies and mitigating their eventual effects, indicating immediate actions and progressive improvement measures, with their respective indicators, controls and documentation.

Likewise, relevant operators shall regularly submit their telecommunication networks and systems to security tests, with the appropriate frequency according to the risk plan approved and sanctioned by their senior **management**. Testing may be carried out by operators internally, or with assistance from external third parties specialised in such services, with the option of requesting the cooperation and advice of the competent cyber-security authority. In any case, they shall be carried out in accordance with up-to-date national or international standards or criteria widely accepted by the telecommunication industry. A record shall be kept of the tests performed, the standards applied, the results obtained, and the action taken as a result.

Security tests and cyber-security drills shall consider, at a minimum, the following control and documentation activities:

- ✓ Updating of the latest version of the Risk Management Plan.
- ✓ Identification and ordering of technical measures for risk management.
- ✓ Development of the set of security tests to be carried out, identifying the physical and logical infrastructure to be used.
- ✓ Physical and logical infrastructure to be used.
- ✓ Detailed description of each test or simulation, the execution procedure and the evidence or means of verification of satisfactory completion of the tests.
- ✓ Detailed description of the restoration activities or measures and procedures for operational and service continuity.
- ✓ Verification of the consistency and security of the storage of logs or records containing cyber-security incidents and other data such as addresses, ports, applications, contents, transmitted data, messages of the systems under test or simulation of cyber-attack or cybersecurity incident.

- ✓ Prepare a report with the result of the security tests or simulations, with appropriate means of verification.

The DGCA, directly or through the body designated for this purpose, may request from the relevant operators all information about the networks and systems they use that is necessary to assess their vulnerability, including their risk management plan, the results of security tests and, in general, all other background information related to security policies for their networks and systems.

Title X, Final provisions

15. Auditing

16. Sanctions

17. Entry in force

CHANGE CONTROL

Date	Version	Created by	Pages modified	Description