NACC/DCA/11 — WP/28 **Rev.**
06/06/23

Eleventh North American, Central American and Caribbean Directors of Civil Aviation Meeting (NACC/DCA/11)
Varadero, Cuba, 28-30 June 2023

Agenda Item 4: **NAM/CAR Regional Safety/Air Navigation Implementation**
4.2 Air Navigation Implementation Matters
Agenda Item 5: **NAM/CAR Regional Aviation Security/Facilitation Implementation**

CYBERSECURITY INITIATIVES – COCESNA

(Presented by Belize, Costa Rica, El Salvador, Guatemala, Honduras and Nicaragua)

EXECUTIVE SUMMARY	
Publicize the main activities implemented by COCESNA in terms of Cybersecurity.	
Action:	Suggested actions are presented in Section 5.
Strategic Objectives:	• Strategic Objective 1 – Safety • Strategic Objective 2 – Air Navigation Capacity and Efficiency • Strategic Objective 3 – Security & Facilitation • Strategic Objective 4 – Economic Development of Air Transport • Strategic Objective 5 – Environmental Protection

1. Introduction

1.1 The purpose of this document is to publicize the main initiatives that COCESNA has undertaken in the field of Cybersecurity.

2. Cybersecurity initiatives

2.1 In terms of cybersecurity, COCESNA began with the establishment of a Specific Objective within the PEC aimed at **"Implementing Cybersecurity in accordance with good practices in the aeronautical and technological sector"**, integrated as part of the strategic objective of "Strengthening the position as a specialized organization in the provision of international aeronautical services". The purpose is to transmit the relevance that COCESNA assigns to the subject, incorporating initiatives aimed at its implementation which are presented in **Illustration 1.**

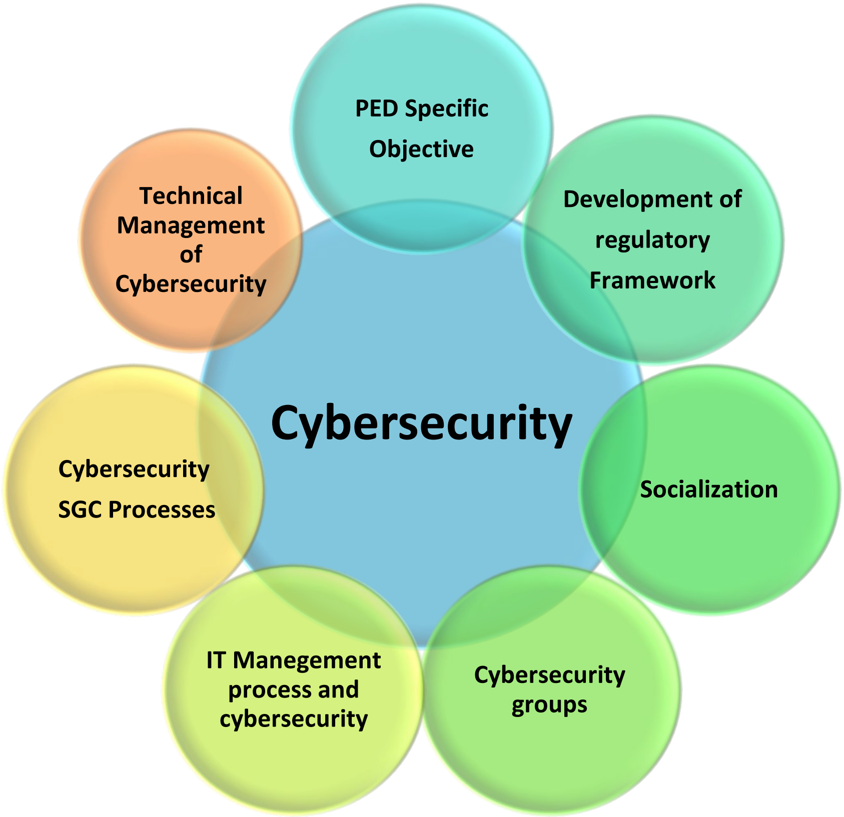

PED Specific Objective
Development of regulatory Framework
Technical Management of Cybersecurity
Cybersecurity
Cybersecurity SGC Processes
Socialization
IT Manegement process and cybersecurity
Cybersecurity groups

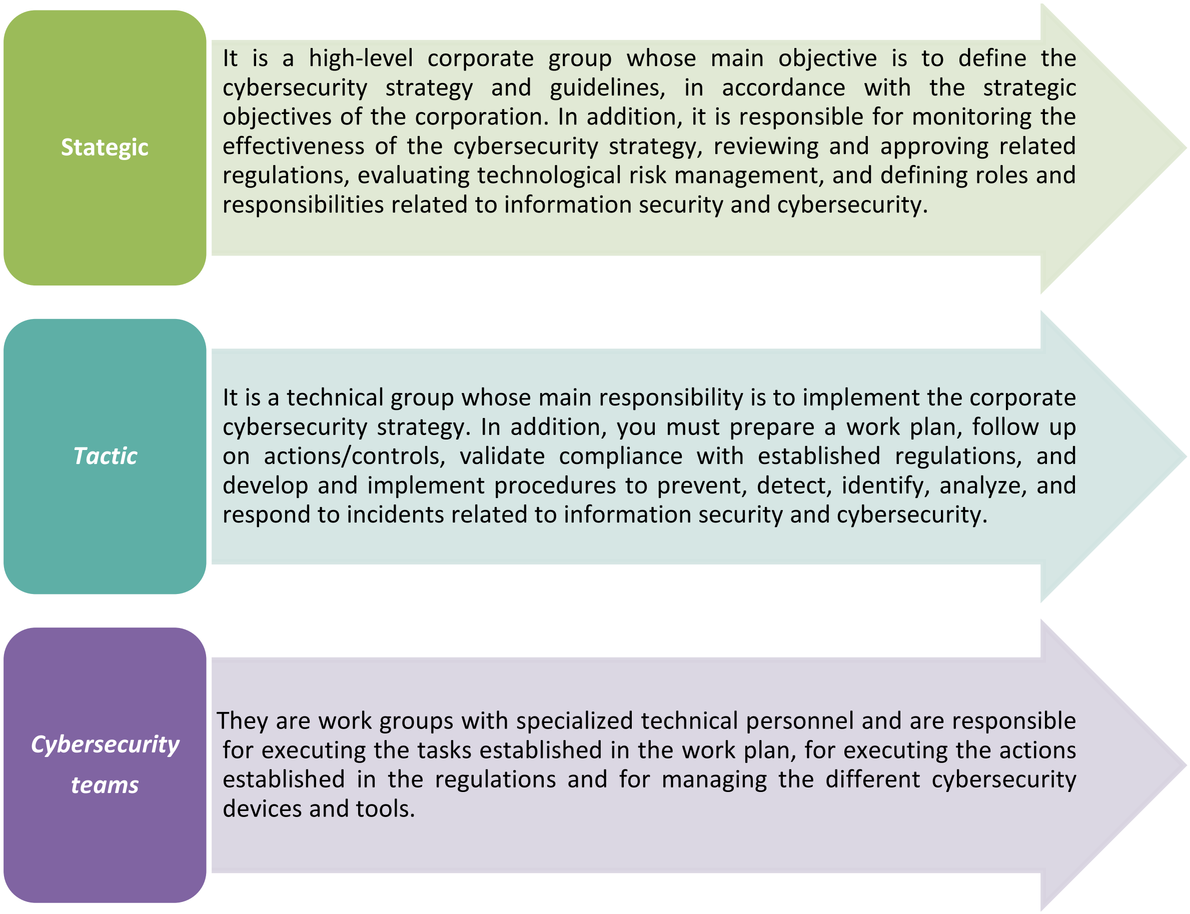
Illustration 1 - COCESNA Cybersecurity Management

2.2 The initiatives undertaken by COCESNA regarding Cybersecurity are detailed below:

a) **Regulatory Framework**: A regulatory framework on cybersecurity was developed, in which the baseline of management at the corporate level was established, and which includes the following:
   - Principles of Information Technology and Cybersecurity,
   - Information Technology and Cybersecurity Management Manual (MGTI),
   - Information Technology and Cybersecurity Policies (PTIC).

b) **Socialization**: Considering that most cybersecurity incidents are caused by human factors, the training of collaborators' competencies was established within the action initiatives. Initially, the regulatory framework was disseminated, later at the level of periodic bulletins on indicators and eventual bulletins with cybersecurity recommendations.

c) **Cybersecurity Groups**: Working groups were established for the implementation of cybersecurity initiatives at the corporate level, which are described in **Illustration 2**.



Stategic

It is a high-level corporate group whose main objective is to define the cybersecurity strategy and guidelines, in accordance with the strategic objectives of the corporation. In addition, it is responsible for monitoring the effectiveness of the cybersecurity strategy, reviewing and approving related regulations, evaluating technological risk management, and defining roles and responsibilities related to information security and cybersecurity.

Tactic

It is a technical group whose main responsibility is to implement the corporate cybersecurity strategy. In addition, you must prepare a work plan, follow up on actions/controls, validate compliance with established regulations, and develop and implement procedures to prevent, detect, identify, analyze, and respond to incidents related to information security and cybersecurity.

Cybersecurity teams

They are work groups with specialized technical personnel and are responsible for executing the tasks established in the work plan, for executing the actions established in the regulations and for managing the different cybersecurity devices and tools.

Illustration 2 - COCESNA Cybersecurity Groups

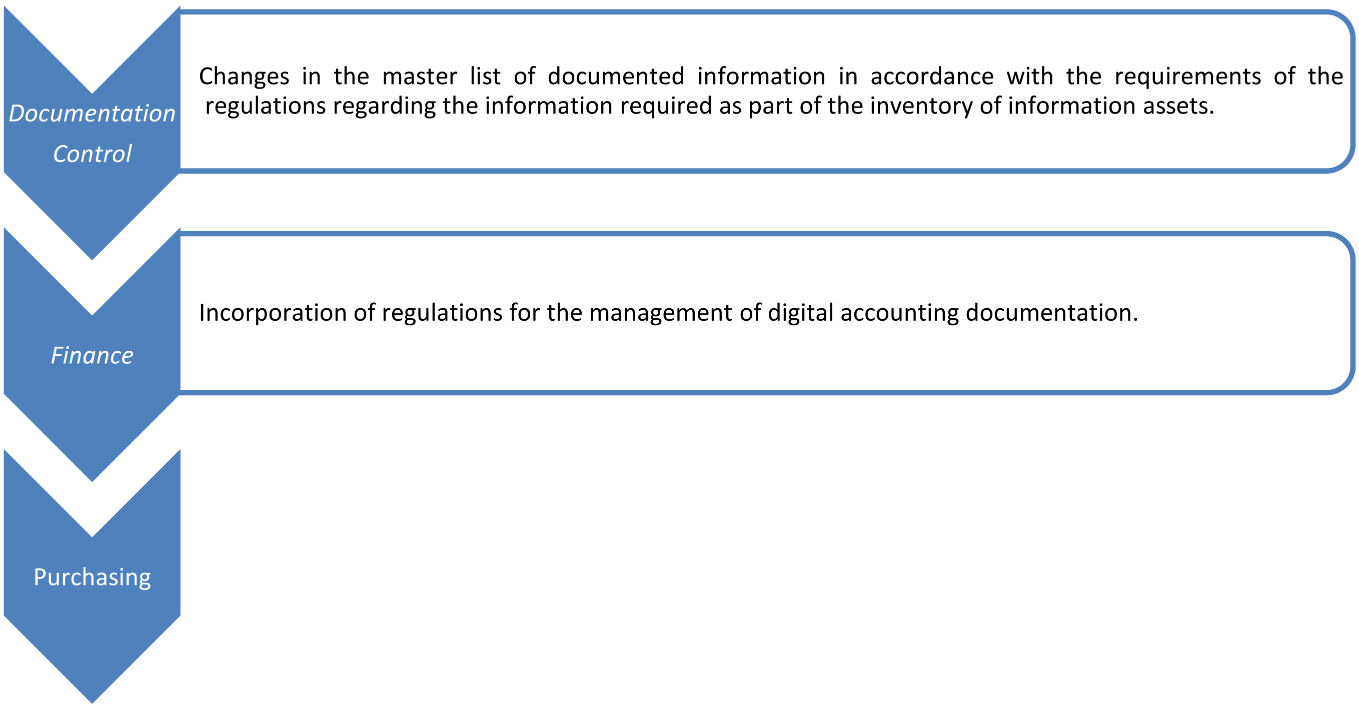
d) **IT and Cybersecurity Management Process:** A process was developed in which the procedures, routines, formats, instructions, and others were established for the administration of IT management and cybersecurity at the corporate level. In addition, these were integrated into the SGC. Among the main activities that were regulated within the process are:

- IT Asset Management;
- IT Data Backup;
- Web services;
- Vulnerabilities and IT Patches;
- IT Logical Access Management;
- Malware Management;
- IT Contingency Plans;
- Signatures on Electronic Documents;
- Risk management in Cybersecurity;
- Awareness in cybersecurity;
- IT incident management;
- Transfer of Information Assets;
- SLA update.

e) **Cybersecurity in OT Process Management:** The OT infrastructure is the technological pillar of the organization, composed of interconnected OT equipment and systems, which constitute the fundamental support for the ATM system and for operations. The following activities and initiatives are being carried out in COCESNA's OT environment to mitigate cybersecurity threats as much as possible and improve the protection of the Operational Technology (OT) infrastructure:

- Internal / external audits of Cybersecurity in CNS / ATM Systems;
- Participation in Cybersecurity groups;
- Analysis of applications used in the OT environment
- Implementing the Password Manager tool
- Implementation of cybersecurity policies for remote access to OT equipment.
- Implementation of Storage Device Use Policies in the OT environment.
- Administration and monitoring of the Access Network
- Access Network Segmentation at the logical level

f) **SGC(QMS) Processes**: Considering that cybersecurity is an integral element within Corporate management, an analysis was carried out and a series of cybersecurity elements were established that should be integrated into the processes already established in the QMS, among which we can highlight those presented below in **Figure** 3



Changes in the master list of documented information in accordance with the requirements of the regulations regarding the information required as part of the inventory of information assets.

Incorporation of regulations for the management of digital accounting documentation.

Illustration 3 - SGC processes

g) **Technical Cybersecurity Management:** It refers to the application of technical measures in the administration of devices and specialized tools for compliance with the regulatory framework, among which we can highlight:

- *Technological Risk Management:* It is related to the evaluation of risks and the application of measures to guarantee the continuity of operations, such as:
  - ✓ Contingency and continuity plans;
  - ✓ Alternate site infrastructure;
  - ✓ Periodic testing of contingency and continuity plans;
  - ✓ Data Backup.

- *Cybersecurity infrastructure:* It is related to the technical administration of cybersecurity devices and tools, such as (not limited to)
  - ✓ Antivirus;
  - ✓ Antispam;
  - ✓ Firewall;
  - ✓ Web Application Firewall (WAF);
  - ✓ Vulnerability scanning;
  - ✓ Video surveillance;
  - ✓ Remote support;
  - ✓ Data encryption;
  - ✓ Secure Erase.

- *IT asset management:* Related to the administration of technological equipment and devices that includes:
  - ✓ Life cycle of IT assets (Planning, provision, administration, discharge);
  - ✓ Classification of IT assets;
  - ✓ Identification of critical assets;
  - ✓ Hardware inventory;
  - ✓ Inventory and allocation of Software licenses;
  - ✓ Patch management.

- • *Logical access control:* Related to account and access management, both for collaborators and external entities, managing the elements presented in **Illustration 4.**

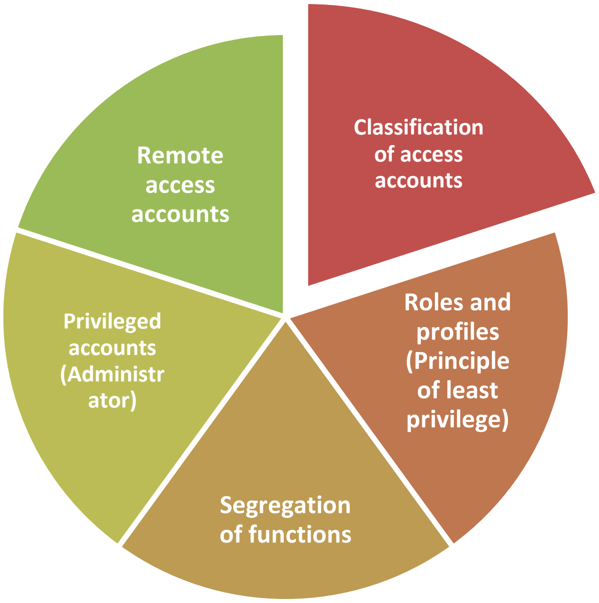


Illustration 4 - Logical Access Management in COCESNA

- *Cybersecurity awareness:* Related to the training of the corporation's personnel, which includes, among other tasks:
  - ✓ Induction (New staff, current collaborators, external entities);

- ✓ Announcements (Newsletters, presentations, talks, Intranet publications);
- ✓ Level of training: Permanent evaluation of the skills required in each job in cybersecurity;
- ✓ Training in Cybersecurity (Trainings, conferences, working groups, consultancies, subscriptions/memberships).

- *Cloud technologies:* Related to industry trends on the provision of Web services and their secure application in COCESNA, among which stand out:
  - ✓ Aeronautical cloud: Provision of SIAREV SaaS (Software as a Service).
  - ✓ Contracted services (Office 365, cloud storage, collaborative work, Web page, quality management SW, social networks, among others).
  - ✓ Hybrid Cloud: Integration between On-Premises services or private cloud (On site with its own infrastructure) with Web services or public cloud.
  - ✓ Evaluation of Cloud service models for SAP Systems.

- *Help Desk:* It is associated with the automation of the management of requests and incidents, in accordance with the best practices, as well as the generation of statistics to support decision-making at the corporate level.
  Illustration 5 presents the various elements that are managed through the COCESNA help desks.

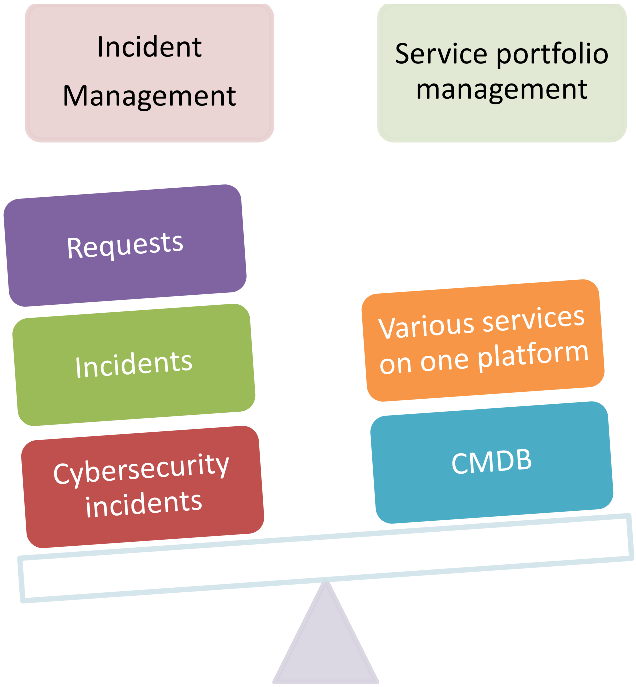


Illustration 5 - COCESNA Help Desk (CATI)

3. Suggested Actions

a) Take into account the initiatives undertaken by COCESNA for the implementation of cybersecurity at the Corporate level;

b) Guide States and Organizations on the development of policies, goal setting, and development of plans that promote cybersecurity in aviation; and

c) Promote the sharing of lessons learned, and the benefits obtained with their implementations for the benefit of other States and organizations.

— END —