Organización de Aviación Civil Internacional
Oficina para Norteamérica, Centroamérica y Caribe

NOTA DE ESTUDIO

NACC/DCA/12 — WP/16
03/07/24

Twelfth Meeting of Directors of Civil Aviation of North America, Central America and the Caribbean (NACC/DCA/12)
Placenta, Belize 09-11 July 2024

Agenda Item: 3 **Aviation Security (AVSEC) and Facilitation (FAL)**

Initiatives of Cybersecurity

(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 – Operational Security • Strategic objective 2 – Air navigation capacity & efficiency • Strategic objective 3 – Aviation security & facilitation • Strategic objective 4 – Economic development of air transport • Strategic objective 5 – Environmental protection
References:	• Specific objective on cybersecurity of COCESNA

1. Introduction

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

2. COCESNA Cybersecurity Axes

Cybersecurity at COCESNA will be supported by three main axes and integrated with each other for the adequate protection of the COCESNA technological platform and its electronic components, which they are presented in **Illustration 1**.

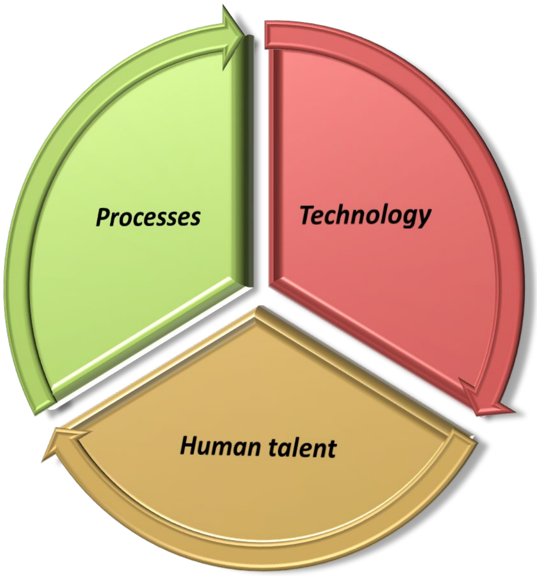


Illustration 1 - COCESNA Cybersecurity Axes

a) **Human Talent**: Strengthen competencies in cybersecurity issues for officials and employees involved in the provision of services.

b) **Processes**: Preparation of guidelines, manuals, procedures, among others, as well as the adoption and adaptation of best practices that allow regulating, controlling and monitoring cybersecurity within the Corporation.

c) **Technology**: Strengthen the life cycle of cybersecurity management with the use of technological tools that allow efficient fulfillment of the functions of identification, protection, detection, response and recovery against possible cyber threats.

3. Cybersecurity initiatives

In terms of cybersecurity, COCESNA began with the establishment of a Specific Objectivewithin 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 2.**

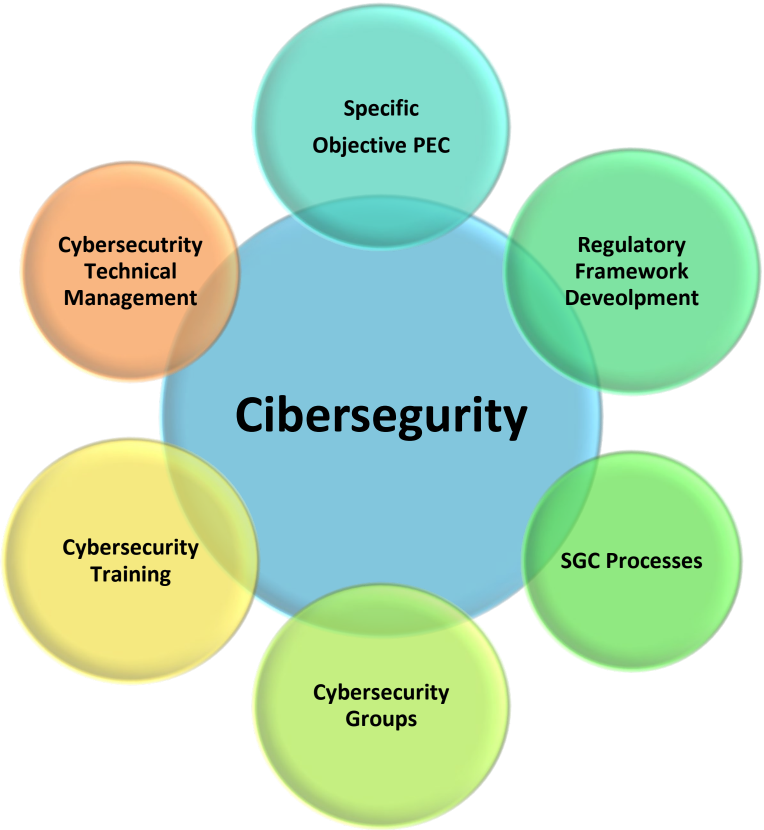


Illustration 2 - COCESNA Cybersecurity Management

The initiatives undertaken by COCESNA regarding Cybersecurity are detailed below:

a) **Specific Objective PEC**: As part of COCESNA's commitment to strengthening cybersecurity, a specific objective related to the implementation of Cybersecurity in accordance with good practices in the aeronautical and technological sector has been established within the COCESNA Strategic Plan (PEC) 2020-2025, within the which frames the initiatives and activities undertaken by COCESNA in terms of cybersecurity.

b) **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).

c) **SGC (QMS) Processes**: Considering that cybersecurity is an integral element within Corporate management, an analysis was carried out and a series of activities were executed out to strengthen COCESNA's QMS, such as:

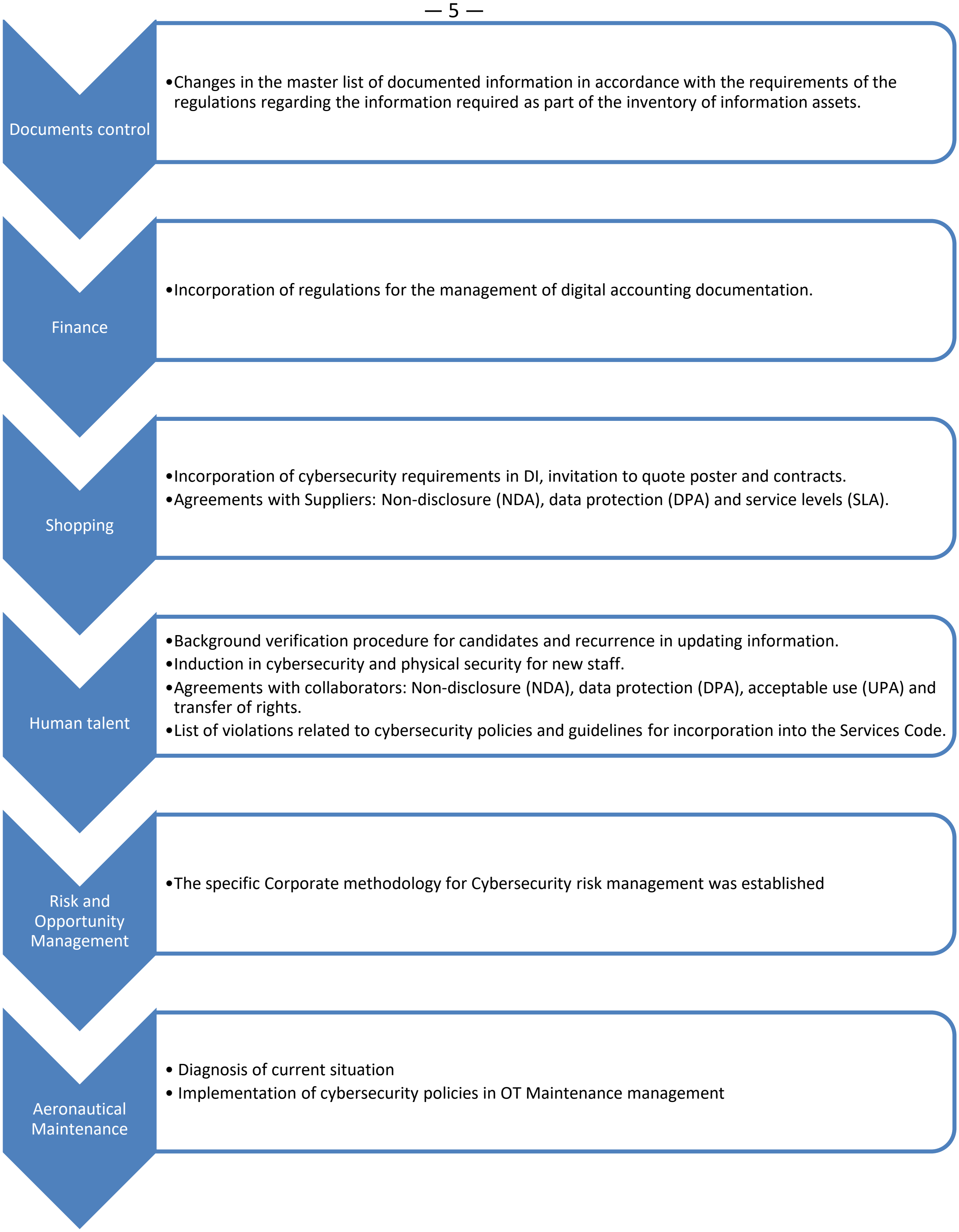
   i. **Cybersecurity in OT Process Management**: The Operational Technology (OT) infrastructure is the technological pillar of the organization, composed of interconnected OT equipment and systems, which constitute the fundamental support for the ATM system and for operations. The following activities 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 OT infrastructure:

- Internal / external audits of Cybersecurity in CNS / ATM Systems.
- Participation in Cybersecurity groups.
- Analysis of software and applications used in the OT environment.
- Implementing privileged accounts Manager tool.
- Implementation of cybersecurity policies for remote access to OT equipment.
- Implementation of Storage Device Use Policies in the OT environment.

ii. **Cybersecurity in IT Process Management**: A process was developed in which the procedures, routines, formats, instructions and others for the administration of IT and cybersecurity management at the corporate level were established, in addition, these were integrated into the Integrated management System of COCESNA (SGS) which is based on QMS. Among the main activities that were regulated within the process are:

- IT Asset Management;
- IT Data Backup;
- Web Services;
- IT Vulnerabilities and Patches;
- IT Logical Access Management;
- Malware Management;
- IT Contingency Plans;
- Signatures on electronic documents;
- Risk Management in Cybersecurity;
- Cybersecurity Awareness;
- IT incident management;
- Transfer of Information Assets;
- Update of SLA with interested parties.

iii. **Other Processes:** In addition to the development or strengthening of specific cybersecurity processes at the OT/IT technical level, considering that cybersecurity is an integral element in Corporate management, a series of cybersecurity elements were identified and incorporated into other QMS processes, among which we can highlight those presented below in **Illustration 3**.



Documents control

- 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.

Finance

- Incorporation of regulations for the management of digital accounting documentation.

Shopping

- Incorporation of cybersecurity requirements in DI, invitation to quote poster and contracts.
- Agreements with Suppliers: Non-disclosure (NDA), data protection (DPA) and service levels (SLA).

Human talent

- Background verification procedure for candidates and recurrence in updating information.
- Induction in cybersecurity and physical security for new staff.
- Agreements with collaborators: Non-disclosure (NDA), data protection (DPA), acceptable use (UPA) and transfer of rights.
- List of violations related to cybersecurity policies and guidelines for incorporation into the Services Code.

Risk and Opportunity Management

- The specific Corporate methodology for Cybersecurity risk management was established

Aeronautical Maintenance

- Diagnosis of current situation
- Implementation of cybersecurity policies in OT Maintenance management

Illustration 3 - Cybersecurity elements of the COCESNA QMS processes

iv. **NIST Diagnosis**: COCESNA will carry out an evaluation of the effectiveness of the controls implemented for the protection of Cyber Threats against critical systems, which is based on the NIST management framework, through which the five domains (as it shows in **Illustration 4)** of the Standard will be verified. with their respective controls.

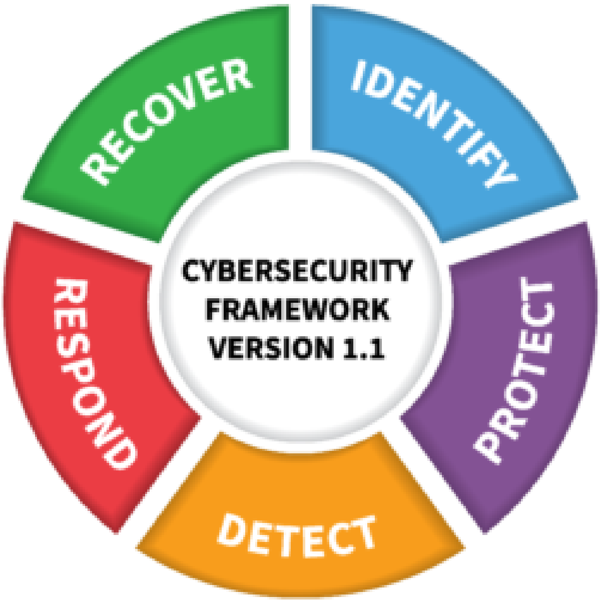


Illustration 4 - NIST Cybersecurity Framework Version 1.1

- **Identify**: Define and document the different systems that the corporation has according to their criticality based on the data and operation of each one for the operation and functioning and availability of COCESNA's operational activities, identifying cybersecurity risks according to access, data, assets and suppliers involved.

- **Protect**: Verify the access levels in the different systems and the cybersecurity measures implemented (firewall, WAF, encryption, among others) as well as the maintenance processes, system and application patching that are executed to contain cybersecurity events.

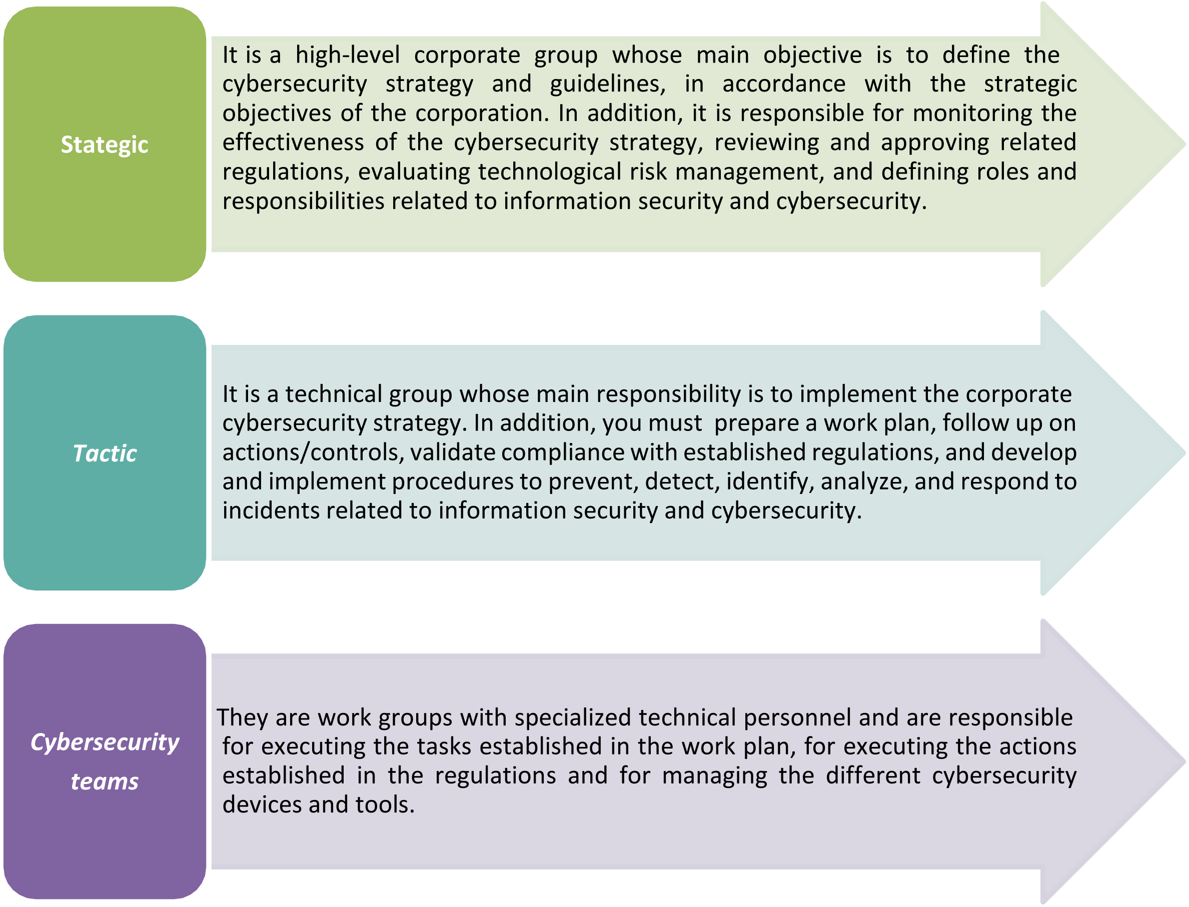
- **Detect**: Validate the correct monitoring of all systems in a timely manner and the configuration of the different alerts of all suspicious activity, ensuring that all stakeholders are informed, validating the corporation's regulatory frameworks and best technological practices, as well as improvements at the configuration level or other applied.

- **Respond**: Investigate the response plans for the different types of incidents that have been mapped, the activities carried out to prevent the spread of an event by mitigating its effects and the subsequent analyzes to execute corrective actions for continuous improvement.

- Recover: Verify incident recovery processes and procedures, ensuring the COCESNA’s reputation.

To apply the developed evaluation form, an activity related to the validation cybersecurity controls effectiveness will be incorporated into the technical supervision visits, to subsequently model the results of the verifications and the evidence collected, to establish a plan of action with activities, responsible persons, resources and investments required to increase the level of maturity of the NIST framework in the Corporation.

d) **Cybersecurity Groups**: Working groups were established for the implementation of cybersecurity initiatives at the corporate level, which are described in **Illustration 5**.



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 5 - COCESNA Cybersecurity Groups

e) **Cybersecurity Training**: Considering that the majority of cybersecurity incidents are caused by human factors, COCESNA has identified the need to train its employees and strengthen their cyber competencies with the objective of establishing a cybersecurity culture at the corporate level, to which a series of activities have been carried out such as:

i. **Socialization**: Initially, the regulatory framework was socialized, with a series of presentations and the participation of all the Corporation's staff.

ii. **Newsletters**: COCESNA has implemented periodic bulletin, presentations, talks, and Intranet publications on cybersecurity recommendations and threat indicators.

iii. **Cybersecurity awareness**: related to the training of the Corporation's personnel, which includes, among other tasks:

- **Induction**: New staff, current collaborators, external entities, this includes the development of specific regulations related to personnel cybersecurity induction activities;

- **Level of training**: Permanent evaluation of the competences required in each job in the field of cybersecurity;

- **Cybersecurity Training**: Formal training, conferences, working groups, consultancies, subscriptions and memberships;

- **Customized courses**: COCESNA is in the process of developing specific cybersecurity material and training to strengthen the cybersecurity skills of its staff.

Illustration 6 shows the activities that COCESNA has initiated as part of Cybersecurity training to achieve a cybersecurity culture at the corporate level.

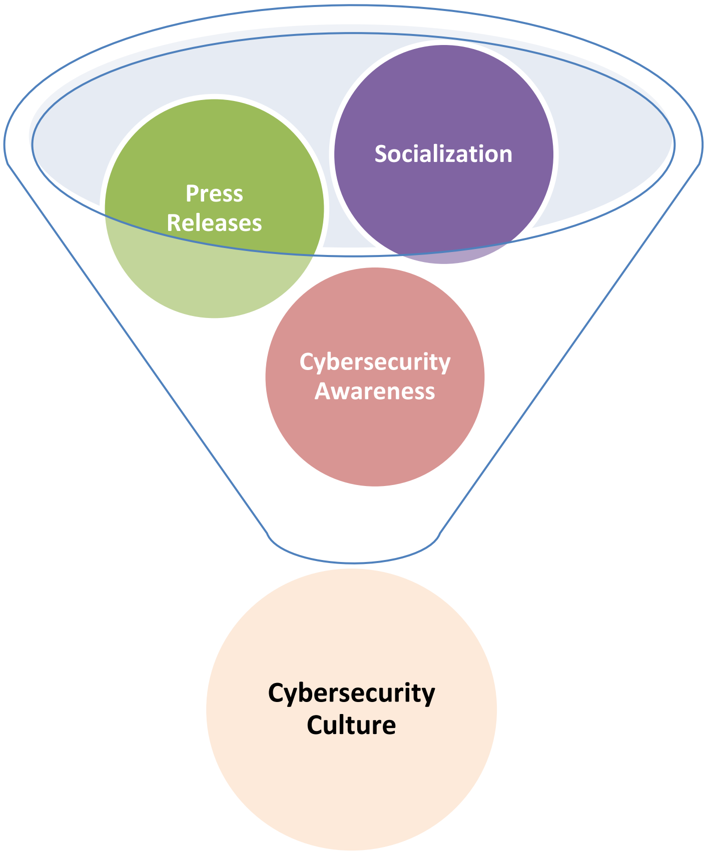


Illustration 6 - COCESNA Cybersecurity Training

f) **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:

i. **SOC**: COCESNA is carrying out a market investigation for the contracting of cybersecurity operations center (SOC) services for the monitoring and protection of critical infrastructure, the attention of cybersecurity incidents and forensic analysis.

ii. **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.

iii. **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.

iv. **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.

v. **Communication Platform Modernization**: One of the main initiatives COCESNA undertook at a technical level is updating the communication infrastructure to provide aviation navigation services, focused especially on strengthening cybersecurity functionalities.

The **Illustration 7** shows the main cybersecurity elements to consider in the communication platform modernization.

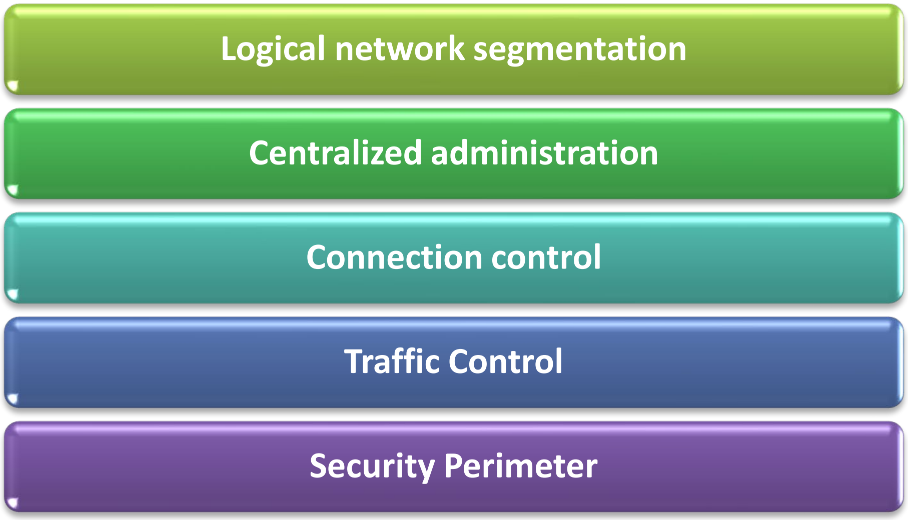


Illustration 7 - COCESNA Communication Platform Modernization

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

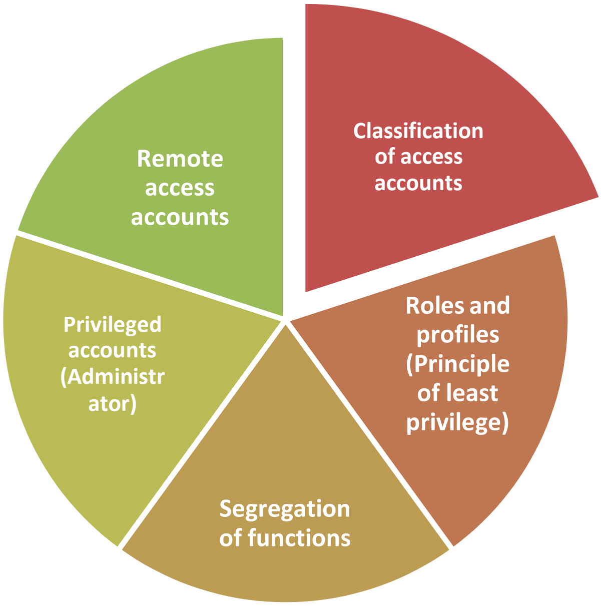

Classification of access accounts
Roles and profiles (Principle of least privilege)
Segregation of functions
Privileged accounts (Administr ator)
Remote access accounts

Illustration 4 - Logical Access Management in COCESNA

vii. *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).

viii. *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.

ix. *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.

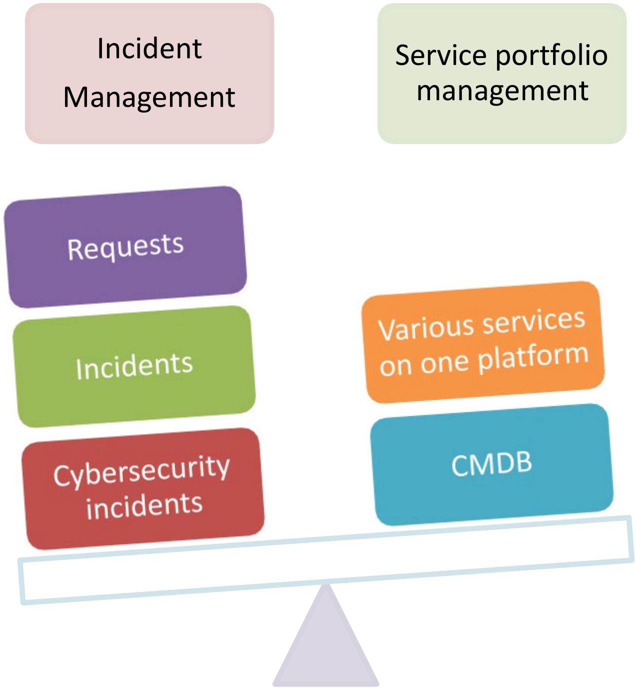


Illustration 5 - COCESNA Help Desk (CATI)

4. 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 —