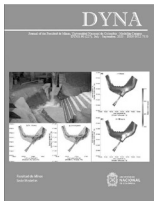
DYNA
http://dyna.medellin.unal.edu.co/



UNIVERSIDAD NACIONAL DE COLOMBIA

Aeronautic maturity cybersecurity: a framework

Guillermo Brito-Acuña

Empresa Cubana de Navegación Aérea, La Habana, Cuba. guillermo.brito@aeronav.avianet.cu

Received: February 23th, 2023. Received in revised form May 25th, 2023. Accepted: June 9th, 2023.

Abstract
This article presents the results of a systematic review of the methods to implement cybersecurity maturity. Based on them, it proposes a framework for excellence in aeronautical cybersecurity that integrates the objectives of aeronautical cybersecurity with capabilities and requirements, which contributes to increasing the maturity of aeronautical cybersecurity. It exposes 13 objectives with 120 capabilities and 5 functional maturity levels to gradually meet up to 600 aeronautical cybersecurity requirements. Which were taken from articles with good practices associated with publications of the last 5 years and the criteria resulting from the collaboration of managers and the validation of experts in the industry, which allowed it to be enriched with good practices associated with the management of cybersecurity and the resilience of these infrastructures.

Keywords: cybersecurity; maturity; aeronautics; framework.

Madurez en ciberseguridad aeronáutica: un marco de trabajo

Resumen
Este artículo presenta los resultados de una revisión sistemática a los métodos para implementar madurez en ciberseguridad. A partir de ellos propone un marco de trabajo para la excelencia en ciberseguridad aeronáutica que integra los objetivos de ciberseguridad aeronáutica con capacidades y requerimientos, lo que contribuye a elevar la madurez de la ciberseguridad aeronáutica. Expone 13 objetivos con 120 capacidades y 5 Niveles funcionales de madurez para gradualmente cumplir hasta 600 requerimientos de ciberseguridad aeronáutica. Las cuales fueron tomadas de artículos con buenas prácticas asociadas a publicaciones de los últimos 5 años y el criterio resultado de la colaboración de directivos y la validación de expertos en la industria, lo que permitió se enriqueciera el mismo con buenas prácticas asociadas a la gestión de la ciberseguridad y la resiliencia de estas infraestructuras.

Palabras clave: ciberseguridad; madurez; aeronáutica; marco de trabajo.

1 Introduction

The need for cybersecurity is widely accepted, both by countries, companies or organizations, regardless of their size. In the aviation industry, the issue takes effect with Resolution A39-19, Direction of Cybersecurity in Civil Aviation [1] recognizing that the global aviation system is a highly complex and integrated system with critical information and technologies that depend on the availability, integrity and confidentiality of the data. In view of compliance with the ICAO established improvement plan until 2030 [2] and the implementation of the Global Aeronautical Information Management System (SWIM) [3], where it will be exchanged with global stakeholders such as airlines, aircraft, civil and military controllers, etc.

Block 1: Establish a solid Cybersecurity device to support information management.

Block 2: Manage the security, integrity, confidentiality and availability of the information that will allow mitigating the risks of intentional interruption and modification of air traffic management information that is critical to operational safety.

The increase in capabilities using cyber-attacks against information and communications systems and the concern of states regarding the possibility of attacks on the air traffic management system are recognized. Agreeing on the creation of groups of experts, the development of capacities to protect critical information, data technology and increase the resilience of the infrastructure, guaranteeing its maintainability and development. To this end, in 2020,

How to cite: Brito-Acuña, G., Aeronautic maturity cybersecurity: a Framework. DYNA, 90(227), pp. 24-34, July - September, 2023.

CANSO published the standard of excellence in cybersecurity for air navigation services, supported by the practices proposed in NIST CSF, endorsed by the experience of its implementation in the European Union [5-7]. This presents a strategy for the continuous improvement of ANSP cybersecurity based on criteria of capacity and maturity (excellence).

This article is organized as follows: section II presents the results of the systematic review; section III presents the framework proposal for excellence in aeronautical cybersecurity that integrates the specific objectives of aeronautical cybersecurity with capabilities and requirements, contributing to raising the management of maturity in aeronautical cybersecurity. 13 objectives with 120 capabilities and 5 maturity levels are exposed to obtain 600 requirements broken down by maturity stages; in section IV the conclusions are presented.

2 Review of the state of the art

During the systematic review, the following terms that identify the research areas were considered: information security management system maturity, maturity cybersecurity and capability maturity cybersecurity. Among the selected sources are specialized databases such as IEEE, Science Direct, SpringerLink and Wiley Online Library. As a result, 28,138 publications regarding maturity in cybersecurity between 2018 and 2022 were analyzed. Of these, a group of 352 articles were considered relevant, identifying 23 primary articles within them. These articles, according to the Petersen criteria, were classified as: Solution proposals (Kour, Karim, Thaduri, & Transit, 2020), Evaluation searches (Kour et al., 2020), Opinion articles (Kour et al., 2020), Experience articles (Kour et al., 2020) and Philosophical articles (Kour et al., 2020). From their analysis, the following observations are made:

1. The non-standardization of the terms is maintained since each author uses different vocabularies for the same meaning.
2. The supremacy of the COBIT model for IT governance issues [29]. A tendency to use it in conjunction with other standards associated with cybersecurity such as ISO 27000 or NIST CSF was identified.
3. Although it is still a developing area, a moderate increase has been identified in the creation of models or frameworks more adapted to their realities, be in industries, institutions or countries. Mainly adapting existing models or creating new models and frameworks. Such is the case of airports, health, banking, the cloud or SCADA systems.
4. The concept of frameworks for maturity in cybersecurity has appeared in the literature. These are practical implementations of existing maturity models or concrete applications on specific areas. Although the use of the framework or model nomenclature is more conditioned to the area where it is developed since in its structure they do not present differences.
5. Both the models and the frameworks present objectives that are traceable to cybersecurity standards. Those, in turn, can be divided into capabilities that establish metrics, controls, or requirements.
6. It is observed that security controls when related to maturity levels only influence the way the process or control is carried out (depending on the characteristics of the level). Without establishing new cybersecurity requirements. Although there are models [10,20] where the complexity of the security requirements increases as a function of level maturity.
7. A small improvement is identified in the tools used to implement the models or frameworks. Where the main tools for its implementation and easy management are developed in MS-Excel files [20,21] although there are others that do it through applications for specific domains [8].
8. Several models [30-33] link organizational resilience to cybersecurity and define that cybersecurity requirements must be supported by good practices and standards associated with the area of competence.

3 Aeronautic cybersecurity framework

For the development of the proposal, the implementation of a framework is considered, seen as a broad overview or scheme of interconnected elements, which defines a standardized set of concepts, practices and criteria to focus on a particular type of problem [30,31]. They provide a base structure to organize the components of a process [34], including capabilities, rules and methods applicable to any scenario regardless of its size or complexity [35]. They define three levels of application from three perspectives: the executive, business process managers, and operations managers [36,37]. This will maintain the structure proposed in the standard for excellence in cybersecurity proposed by Canso, to which the capabilities layer was added and, consequently, the requirements layer was expanded.

Fig. 1 exposes the simplified structure of the framework and the traceability between COBIT, NIST CSF, the standard for excellence in aviation cybersecurity [38], proposed by CANSO. It exposes 13 objectives, 120 capabilities and 5 maturity levels to obtain 600 maturity requirements.

3.1. Standard ratio and tired goals

Regarding the cybersecurity standards that the framework respects, those recommended by CANSO, that is, COBIT and NIST CSF will be maintained. COBIT for its results in the management of IT governance will be traceable with the Objectives:

1. Leadership and Governance: Where senior management demonstrates leadership and commitment to cybersecurity. Policies necessary to manage and monitor regulatory, legal, risk, environmental, and operational requirements related to cybersecurity are approved and help ensure that cybersecurity supports business objectives, optimizes business investment, and appropriately manages risks and opportunities related to cybersecurity.
2. Cybersecurity Management System: Where the elements that establish security policies, processes and objectives are related. Through a culture of security, it fosters

cooperation between stakeholders, manages threat and risk assessment, and acts as an independent party to provide advice, audit systems and processes without having a direct role in the operation.

3. NIST CSF for its part will be traceable to the objectives:
4. Asset Management: Where the data, personnel, devices, systems and facilities that allow the organization to achieve its business objectives are managed according to their relative importance and their risk strategy.
5. Risk Assessment: Where the cybersecurity risk for operations is understood, including the mission, functions, image or reputation, assets and people. It includes managing threats and vulnerabilities and identifying control gaps for areas and managing the assessed risks.

a. Levels and stages of maturity and capability

Regarding the levels of maturity or capacity used in the framework, the following concepts will be added:

Stage: Period of fulfillment of requirements between one level and another.

Level 0) Incomplete: Where the requirements that allow cybersecurity to be considered at level A – Informal are not met.

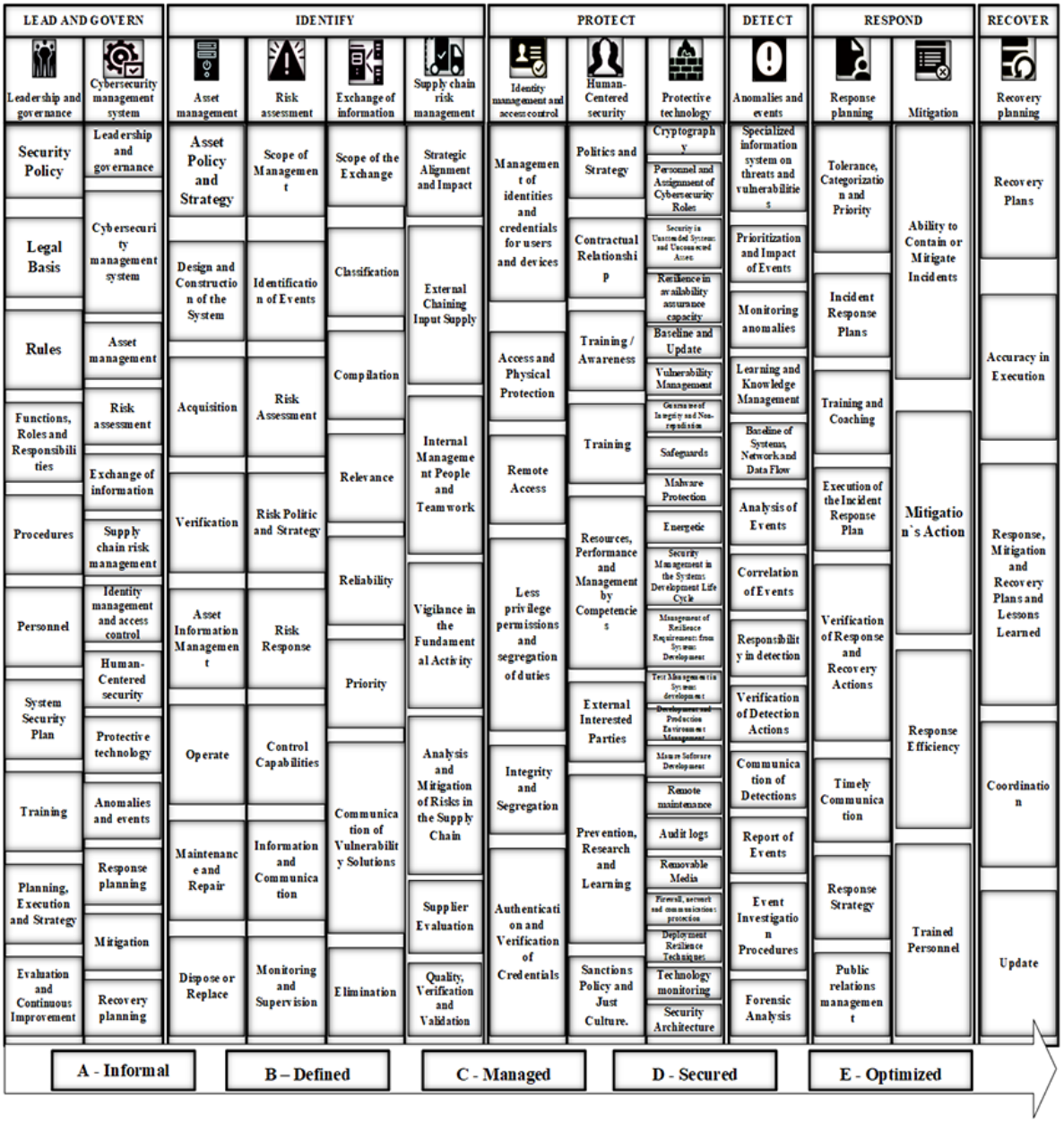


Figure 1. Structure of the framework for aviation cybersecurity maturity.
Source: Own elaboration.

Maintaining the levels proposed by fatigue as follows:

Level 1) A - Informal: Where the requirements are met to a large extent by the expertise of its members.

Level 2) B – Defined: Where compliance with the requirements is indicated and organized with an organizational vision.

Level 3) C - Managed: Where the organization documents the procedures, rules and responsibilities of its actors and establishes mechanisms to meet its goals.

Level 4) D - Secured: Where the cybersecurity results are interpreted through metrics, all the previous stages are consolidated through the automation of processes and formally involve the interested parties.

Level 5) E - Optimized: Where the organization seeks the continuous improvement of its cybersecurity through international practices. The system is able to quickly adapt to changes in terms of threats, vulnerabilities, risks, economic strategy or organizational needs.

1 Identification and validation by experts of the capacities and requirements by level

The foundations for building excellence are obtained by consolidating the requirements based on the level of maturity of the capability. These capabilities are grouped by their objectives, which have been established according to the characteristics of the maturity levels, while increasing their completeness and compliance, strengthened with specific standards, in organizational resilience and good practices identified in the literature. Therefore, knowing the objectives and levels, it was imperative to determine the security and resilience requirements to be implemented, as well as in what capacity to contain it and at what level of maturity.

To determine the requirements, the systematic review of the bibliography, the Delphi method and the focus group were applied as scientific methods The systematic review of the bibliography: Identifies, evaluates and combines the evidence of the primary research studies through an explicit and rigorous method. Being useful to evaluate and interpret relevant information available associated with an investigation [39].

The Delphi method: It is used internationally in several areas of knowledge; its purpose is to socialize, externalize and combine the knowledge of experts under anonymity, enabling the participation of geographically dispersed experts [40].

The focus group: it is a type of group interview to collect opinions and knowledge on a specific topic. Its application stimulates the members to emit ideas about the object under investigation and the interaction between them allows to consider additional aspects or identify common problems [41].

For the identification of requirements, a bibliographic review of standards, models, frameworks and articles on the subject was carried out. This information was enriched by particularizing it to the aeronautical environment with the help of experts, making use of the Delphi method in its first round. The results obtained were submitted to the focus group where the proposal was enriched with real experiences, proposing the capacities, the development of a software for the management of the framework, the Fig. 1. representing the stages and levels of maturity and the extension of the scope to others. standards not directly involved with cybersecurity but implementing them would provide good practices for the resilience of the organization. Finally, the second round of Delphi was applied with the proposal refined in the previous step.

For the systematic review, the one previously carried out in 1.3 was expanded by adding the requirements established in multiple standards and consolidated capacity and maturity models, such is the case of the ISO 27000 family [41], the NIST SP 800 series standards related to NIST Cybersecurity Framework (NIST CSF) Version 2.0 [42] or NIST SP 800-53 rev.5 [43], Cybersecurity Maturity Model Certification (CMMC) Version 2.0 [44], Cybersecurity Capacity Maturity Model for Nations (CMM) [45], Cybersecurity Capability Maturity Model (C2M2) Version 2.1 [46] and the Cybersecurity Framework Version 4.2 [47] implemented in Uruguay [48]. The relevance of the requirements found was validated by identifying recent scientific publications (5 years) that developed the topic.

There were 783 basic cybersecurity practices were determined, which were located at the corresponding maturity level and were developed observing the characteristics of the levels towards which they mature or the data necessary to guarantee their assurance at previous levels. Allowing the emergence and specification of new requirements, supported by the increase in complexity and completeness of said specifications for implementation.

These practices, once the framework has been adopted, are considered requirements for its implementation depending on the level to be reached. The capabilities arose from the accumulation of requirements on a specific capability within each objective. As the existence of few publications that issued clear criteria on requirements, capacities and objectives was identified, it was decided to submit the proposal to the first round of experts.

To apply Delphi and the focus group, it is necessary to identify experts in aeronautical cybersecurity. To this end, the following expert selection criteria were considered [49]:

Having performed roles related to cybersecurity.

More than five years of experience in cybersecurity and more than three years linked to aeronautical cybersecurity.

Having successfully managed improvements in cybersecurity in organizations related to aeronautics or other similar critical infrastructures.

Possess knowledge in the branches of engineering related to critical infrastructures, CNS/ATM, quality management, process improvement, methodologies, models and cybersecurity maturity standards.

Possess publications and industry recognition for their contributions to aeronautical cybersecurity.

For this reason, 27 candidates for experts from both the national industry and other service providers, aeronautical technique producers or international regulatory bodies were contacted. Twenty-one of them agreed to participate and had their curricular synthesis reviewed. Representing 9 organizations (5 Cuban and 8 foreign), with nationality from Cuba (14), Argentina, Chile, Mexico, the Dominican Republic, the Netherlands, the United States and Germany.

Of the 21 experts, 6 whose competence indices were less than 0.5 were dismissed. Out the selected 15 experts, 12 obtained a high competence coefficient and 3 of them medium. Which were characterized to guarantee their quality for research.

Based on the correlation proposal between objectives, capabilities, requirements and levels, the first round of Delphi was carried out to adapt the proposal to the aeronautical context. Carried out through a virtual discussion group, supported by video conference, where the moderator informed that the purpose of the meeting is to identify the cybersecurity capabilities and requirements by level to be implemented in the organizations that ensure aeronautical services. The anonymity and confidentiality of the responses to the survey or criteria that will be obtained at the meeting was guaranteed.

To ensure the understanding of the experts, the moderator explains each objective and the maturity requirements by level, for each capability. In parallel, for each capacity explained, each expert receives a survey in which to assess, according to the Likert scale, their degree of agreement or disagreement, the relevance or otherwise of each capacity or its requirements by level. In addition, it allows you to propose changes for each question. In the first round, the experts proposed a total of 56 changes, which can be summarized in the following items:

They proposed 52 adaptations of requirements that were ahead of the characteristics of the level of maturity. Incorporating specialized standard practices in other capacities that are not exactly cybersecurity, these approaches are supported under the hypothesis that implementing standardized good practices in key capacities will contribute to increasing organizational resilience. And considering the complexity of implementation of the framework, the use of tools for its management.

Considering the results obtained through the expert method, they were submitted to an exploratory focus group, to which industry executives and other interested parties were added, which enriched the proposal with real experiences, also proposing the following recommendations for execution.

Use the ISO 55000 standard in the case of asset management, CMMi for software project development, ISO 28000 for supply chain security management and ISO 22301 for business continuity.

Develop a tool that allows the control of the complete management cycle of the improvements projected by the system of excellence in cybersecurity, which is compatible with the quality management systems and the operational safety management system and which can cover several organizations.

Once the proposal was updated considering the established recommendations, the second round of the survey was carried out. The experts once again gave their consideration on the practices, evidencing a higher level of consensus than in the first round and a greater acceptance of the proposal. The experts valued the use of the recommendations for the implementation of the framework, observing a high concordance with the proposals issued in the focus group (in all cases above 85%). To demonstrate the reliability of the answers given by the experts in the questionnaires, it was necessary to calculate the coefficient of agreement between them.

For the processing of the results of the survey, a method was used that consists of identifying the frequency in each category of the Likert scale defined in the survey and the percentages of concordance of each category are calculated according to the characteristics proposed by the author, then it is calculated in a percentage index, which integrates in a single value the acceptance of the group of evaluators on the characteristics of the model. The percentage index of the experts in each of the questions exceeds the value of 85. Therefore, the processing carried out through the Likert scale shows the acceptance by the community of experts of the objectives, capacities, levels and their requirements, as well as the software presented in support of the management of the framework for excellence in aeronautical cybersecurity.

From these analyses, it was possible to define the correlation between the cybersecurity and resilience requirements based on the level of maturity, for each capacity that makes up each of the objectives proposed in the standard of excellence for air navigation. Functional recommendations were determined that facilitate the management of the complete cycle associated with the necessary improvements to implement the framework and its interrelation with consolidated processes in the industry, such as Quality Management or Operational Safety Management [50].

2 List of objectives, capabilities and specification of requirements by level

Expanding on the results reached in the previous section, the correlation obtained between the objectives, capacities and requirements by level is presented, and references are made to articles found that validate the topicality of the topic.

Within the Leadership and Governance objective, the practices associated with ISO 38500 [51], GCSCC [52], CMM, ITIL and COBIT5 [53] are followed. The proposed capabilities to mature are: 1) Security Policy [54]; 2) Legal Basis [55]; 3) Rules [56]; 4) Functions, Roles and Responsibilities [57]; 5) Procedures [58]; 6) Personnel [59]; 7) System Security Plan [60]; 8) Training [61]; 9) Planning, Execution and Strategy [62] and 10) Evaluation [63] and Continuous Improvement [64].

In the Information Security Management System objective, the practices associated with ISO 27000, 27001, 27003 and 27004 [65] and the Standard of Excellence in Cybersecurity established by CANSO are adapted. As the purpose of this objective is to direct the management, it is proposed to maintain the following capacities 11) Leadership and Governance; 12) Information Security Management System; 13) Asset Management; 14) Risk assessment; 15) Exchange of information; 16) Supply chain risk management; 17) Identity management and access control; 18) Human-Centered Security; 19) Protective technology; 20) Anomalies and events; 21) Response planning; 22) Mitigation and 23) Recovery Planning.

In the Asset Management objective, the practices recommended in ISO 55000, 55001 and 55002 [66] are adapted, proposing the following capabilities: 24) Management Diagnosis [67]; 25) Asset Policy and Strategy

[68]; 26) Design and Construction of the System [69]; 27) Acquisition [70]; 28) Verification [71]; 29) Asset Information Management [72]; 30) Operate [73]; 31) Maintenance and Repair [74] and 32) Dispose or Replace [75].

The Risk Assessment objective responds to the recommended practices in the ISO 31000 family, ISO 27005, NIST SP 800-30 [76] and Cyber Security and Risk Assessment Guide, proposing the following capacities: 33) Scope of Management [77]; 34) Identification of Events [78]; 35) Risk Assessment [79]; 36) Risk Response [80]; 37) Control Capabilities [81]; 38) Information and Communication [82] and 39) Monitoring and Supervision [83].

The Information Exchange objective provides the practices suggested by NIST SP 800-47 and ISO 20614 and ISO 27032 proposing as capabilities: 40) Scope of the Exchange [84]; 41) Classification [85]; 42) Compilation [86]; 43) Relevance [87]; 44) Reliability [88]; 45) Priority [89]; 46) Communication of Vulnerability Solutions [90]; and 47) Elimination [91].

In the Risk Management objective in the supply chain, the practices of ISO 28000 and 28001 are adapted, proposing the capacities: 48) Strategic Alignment and Impact [92]; 49) External Chaining Input Supply [93]; 50) Internal People Management and Teamwork [94]; 51) Surveillance in Fundamental Capacity [95]; 52) Analysis and Mitigation of Risks in the Supply Chain [96]; 53) Evaluation of Suppliers [97] and 54) Quality, Verification and Validation [98].

The Identity Management and Access Control objective complements the practices declared in ISO 29146, NIST SP 800-205 and the ISO 24760 family, for which reason it proposes the following capabilities: 55) Management of identities and credentials for users and devices [99]; 56) Access and Physical Protection [100]; 57) Remote Access [101]; 58) Permits with less privilege and segregation of duties [102]; 59) Integrity and Segregation [103] and 60) Authentication and Verification of Credentials.

The Human-Centered Security objective uses the success factors declared in ISO 27501, ISO 30408, NIST SP 800-181, ICAO Manual 9859 and 10057 and the CANSO Human Resources Management Excellence Model, at the same time that proposes as capacities: 61) Politics and Strategy; 62) Contractual Relationship; 63) Training / Awareness [104]; 64) Training; 65) Resources, Performance and Management by Competencies [105]; 66) External Interested Parties; 67) Prevention, Investigation and Learning [106] and 68) Sanctions Policy and Just Culture.

In the Protective Technology objective, recommended practices are included in NIST SP 800-160, NIST SP 800-40, NIST SP 800-86, CMMi, ISO 62443 data protection [106], the maturity model for web applications against cyber-attacks based on in OSWAP [107], and the Action Plan for the implementation of an ICAO Cybersecurity Strategy, the proposed capabilities are: 69) Cryptography [108]; 70) Personnel and Assignment of Cybersecurity Roles [109]; 71) Security in Unattended Systems and Unconnected Assets [110]; 72) Resilience in capacity to ensure availability [111]; 73) Baseline and Update [112]; 74) Vulnerability Management [113]; 75) Guarantee of Integrity and Non-repudiation [114]; 76) Safeguards [115]; 77) Antivirus Protection [116]; 78) energetic; 79) Security Management in the Systems Development Life Cycle; 80) Management of Resilience Requirements from Systems Development; 81) Test Management in Systems development; 82) Development and Production Environment Management; 83) Mature Software Development; 84) Remote maintenance; 85) Audit logs ; 86) Removable Media [117]; 87) Firewall, protection of networks and communications [59]; 88) Deployment Resilience Techniques [118]; 89) Technology Monitoring [119] and 90) Security Architecture [120].

The Anomalies and Events objective uses the success factors declared in NIST SP 800-92, NIST SP 800-94 and NIST SP 800-137 and the maturity-oriented model in forensic analysis [121] to propose the capabilities: 91) Specialized information system on threats and vulnerabilities; 92) Prioritization and Impact of Events; 93) Monitoring of anomalies [122]; 94) Learning and Knowledge Management [123]; 95) Baseline of Systems, Network and Data Flow; 96) Analysis of Events; 97) Correlation of Events; 98) Responsibility in detection; 99) Verification of Detection Actions; 100) Communication of Detections; 101) Report of Events; 102) Event Investigation Procedures and 103) Forensic Analysis.

The Response Planning objective includes success factors declared in CSFPC, NIST 800-61, ISO 27035, ICAO Doc. 9756 and the CANSO Emergency Response Plan, to present the capabilities: 104) Tolerance, Categorization and Priority; 105) Incident Response Plans [124]; 106) Training and Training [104]; 107) Execution of the Incident Response Plan; 108) Verification of Response and Recovery Actions; 109) Timely Communication; 110) Response Strategy and 111) Public relations management.

The Mitigation objective bases its capabilities on the success factors declared in ISO 22316, ISO 22317 and BSI 65000 proposing: 112) Ability to Contain or Mitigate Incidents; 113) Mitigation Actions; 114) Response Efficiency and 115) Trained Personnel [104].

Finally, the Recovery Planning objective is supported by the ISO 22301, ISO 22313 and ISO 24762 standards, it presents the following capabilities: 116) Recovery Plans; 117) Accuracy in Execution; 118) Response, Mitigation and Recovery Plans and Lessons Learned [125]; 119) Coordination and 120) Update.

Each capacity will present requirements that will gain in completeness and complexity depending on the level of maturity that is intended to be obtained. The levels to be used were those previously explained. Therefore, the framework will have 600 requirements, 120 for each defined level except for the Stage or Incomplete Level where all the minimum requirements have not yet been met to reach level A - Informal.

Each requirement is correlated with a level and with a capacity, these may have 3 states: 1) Pending: When all the requirements proposed for a stage are not met, the organization is not able to provide evidence of compliance and its implementation is not projected. compliance. 2) In process: When the organization has projected its compliance through actions, tasks and the necessary assurance for its compliance. 3) Fulfilled: when the institution is capable of

providing evidence of compliance with all the requirements stipulated in the stage and the level of maturity evaluated. Evidence of compliance will serve as the basis for determining the state of maturity of the organization and a source of comparison between entities. To use the framework, the following constraint is used:

Restriction 1: It is only possible to declare a requirement fulfilled when all the requirements of previous stages are fulfilled.

3 Conclusions

In conclusion, this article has presented a framework for the management of aeronautical cybersecurity maturity, based on a systematic review of publications and enriched with good practices provided by executives and experts in the industry. The framework includes 13 objectives, 120 capabilities, and 5 functional levels of maturity, with a total of 600 requirements that can be used to achieve maturity levels in a certifiable and gradual manner. The framework not only contributes to improving the resilience of aeronautical infrastructures, but also enhances their integration with other management systems such as security, quality, or safety. This framework represents an important step forward in the development and implementation of effective cybersecurity management practices in the aeronautical industry.

References

[1] ICAO, Resolution A41-19: Addressing cybersecurity in civil aviation, Montreal, Canada, 2022. [consultation, May 7, 2023]. Available at: https://www.icao.int/aviationcybersecurity/Documents/A41-19.pdf .

[2] ICAO, 2016 - 2030 Global Air Navigation Plan - ICAO Doc. 9750-AN/963, 5th Edition, Montreal, Canada, 2022. [consultation, May 7, 2023]. Available at: https://www.icao.int/airnavigation/documents/ganp-2016-interactive.pdf

[3] Zhang, X., Zhong, S., and Mahadevan, S., Airport surface movement prediction and safety assessment with spatial–temporal graph convolutional neural network. Transportation Research Part C: Emerging Technologies, 144, art. 103873, 2022. DOI: http://dx.doi.org/10.1016/j.trc.2022.103873

[4] Sridhar, B., and Bell, D., Sustainable aviation operations and the role of information technology and data science: background, current status and future directions. AIAA AVIATION 2022 Forum. 2022. DOI: https://doi.org/10.2514/6.2022-3705

[5] Stroeve, S., Smeltink, J., and Kirwan, B,. Assessing and advancing safety management in aviation. Safety, 8(2), art. 20, 2022. DOI: https://doi.org/10.3390/safety8020020

[6] Yoon, M.G., and Kim, J.K., Evaluation methodology for safety maturity in air navigation safety. Journal of Air Transport Management, 98, e102159, 2022. DOI: https://doi.org/10.1016/j.jairtraman.2021.102159

[7] Jia, Z., and Qi, F., Developing a civil aviation safety management maturity model to promote the safety level of civil aviation. International Journal of Reliability and Safety, 15(4), art. 306, 2021. DOI: https://doi.org/10.1504/ijrs.2021.10050705

[8] Kour, R., Karim, R., and Thaduri, A., Cybersecurity for railways. A maturity model. Proceedings of the Institution of Mechanical Engineers, Part F: Journal of Rail and Rapid Transit, 234 (10), pp 1129-1148, 2020. DOI: https://doi.org/10.1177/0954409719881849

[9] Yigit-Ozkan, B., van Lingen, S., and Spruit, M., The Cybersecurity Focus Area Maturity (CYSFAM) Model. Journal of Cybersecurity and Privacy, 1(1), pp. 119-139, 2021. DOI: https://doi.org/10.3390/jcp1010007

[10] Ghaffari, F., and Arabsorkhi, A., A New adaptive cyber-security capability maturity model. 2018 9th International Symposium on Telecommunications (IST), 2018. DOI: https://doi.org/10.1109/istel.2018.8661018

[11] Almomani, I., Ahmed, M., and Maglaras, L., Cybersecurity maturity assessment framework for higher education institutions in Saudi Arabia. PeerJ Computer Science, 7, e703. Portico, 2021. DOI: https://doi.org/10.7717/peerj-cs.703

[12] Rea-Guaman, A.M., Mejía, J., San Feliu, T., and Calvo-Manzano, J.A., AVARCIBER: a framework for assessing cybersecurity risks. Cluster Computing, 23(3), pp. 1827-1843, 2020. DOI: https://doi.org/10.1007/s10586-019-03034-9

[13] Aliyu, A., Maglaras, L., He, Y., Yevseyeva, I., Boiten, E., Cook, A., and Janicke, H., A holistic cybersecurity maturity assessment framework for higher education institutions in the United Kingdom. Applied Sciences, 10(10), e3660, 2020. DOI: https://doi.org/10.3390/app10103660

[14] Perales-Manrique, J.H., and Molina-Chirinos, J.A., Modelo de madurez de analítica de datos para el sector financiero, 2020. DOI: https://doi.org/10.19083/tesis/652126

[15] Al-Matari, O.M.M., Helal, I.M.A., Mazen, S.A., and Elhennawy, S., Adopting security maturity model to the organizations' capability model. Egyptian Informatics Journal, 22(2), pp. 193-199, 2021. DOI: https://doi.org/10.1016/j.eij.2020.08.001

[16] Schlette, D., Vielberth, M., and Pernul, G., CTI-SOC2M2 - The quest for mature, intelligence-driven security operations and incident response capabilities. Computers & Security, 111, e102482, 2021. DOI: https://doi.org/10.1016/j.cose.2021.102482

[17] Malhotra, O., Dey, S., Foo, E., and Helbig, M., Cyber Security maturity model capability at the airports, ACIS 2021 Proceedings, 55, [online]. 2021. Available at: https://aisel.aisnet.org/acis2021/55

[18] Schmitz, C., Schmid, M., Harborth, D., and Pape, S., Maturity level assessments of information security controls: an empirical analysis of practitioners assessment capabilities. Computers & Security, 108, e102306, 2021. DOI: https://doi.org/10.1016/j.cose.2021.102306

[19] Yigit-Ozkan, B., and Spruit, M., A questionnaire model for cybersecurity maturity assessment of critical infrastructures. Information and operational technology security systems, 2019, pp. 49-60. DOI: https://doi.org/10.1007/978-3-030-12085-6_5

[20] Pérez-Navarro, H.B. y Salcedo-Jara, H.L., Modelo de madurez en ciberseguridad para empresas que manejan datos de salud, [en línea]. 2022. Disponible en: http://hdl.handle.net/10757/655801

[21] Cyber Security - An introduction to assessment and maturity frameworks. An introduction to cyber modeling and simulation, 2018, pp. 9-18. DOI: https://doi.org/10.1002/9781119420842.ch2

[22] Zárate-Santos, I.J., Herramienta de armonización entre las normas 27001 y NIST800-53 como pilares para la medición del nivel de madurez del SGSI, [en línea]. 2022. Disponible en: https://hdl.handle.net/10983/26924

[23] Aristizábal-Correa, J.M., Marín-Ramírez, L., and Álvarez-Salazar, J., Identificación de elementos de seguridad basados en el modelo C2M2 para la industria manufacturera del sector textil. Revista Colombiana de Computación, 20(2), pp. 56-67, 2019. DOI: https://doi.org/10.29375/25392115.3722

[24] Drivas, G., Chatzopoulou, A., Maglaras, L., Lambrinoudakis, C., Cook, A., and Janicke, H., A NIS directive compliant cybersecurity maturity assessment framework. 2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), 2020. DOI: https://doi.org/10.1109/compsac48688.2020.00-20

[25] Dube, D.P., and Mohanty, R.P., Towards development of a cyber security capability maturity model. International Journal of Business Information Systems, 34(1), art. 104, 2020. DOI: https://doi.org/10.1504/ijbis.2020.106800

[26] Maglaras, L., Drivas, G., Chouliaras, N., Boiten, E., Lambrinoudakis, C., and Ioannidis, S., Cybersecurity in the era of digital transformation: the case of Greece. 2020 International Conference on Internet of Things and Intelligent Applications (ITIA), 2020. DOI: https://doi.org/10.1109/itia50152.2020.9312297

[27] Gallardo, J., Torres, R., and Tessini, O., Surveillance platform of cybersecurity maturity of micro and small enterprises. 2020 39th International Conference of the Chilean Computer Science Society (SCCC), 2020. DOI:

https://doi.org/10.1109/sccc51225.2020.9281264
[28] Orellana-Cabrera, X.E., and Álvarez-Galarza, M.D., Marco de trabajo de gobierno de TI orientado a la ciberseguridad para el sector bancario bajo COBIT 2019. Polo del Conocimiento, 7(3), pp. 706-726, 2022. Available at: https://dialnet.unirioja.es/descarga/articulo/8399852.pdf
[29] Akinsanya, O.O., Papadaki, M., and Sun, L., Current cybersecurity maturity models: how effective in healthcare cloud?. In CERC 2019, pp. 211-222. Available at: https://ceur-ws.org/Vol-2348/paper16.pdf
[30] Stastny, P., and Stoica, A.-M., Protecting aviation safety against cybersecurity threats. IOP Conference Series: Materials Science and Engineering, 1226(1), art. 012025, 2022. DOI: https://doi.org/10.1088/1757-899x/1226/1/012025
[31] Olarte-Rojas, A.D., Propuesta metodológica para la evaluación de la madurez del sistema de gestión de continuidad del negocio en el sector financiero bancario colombiano bajo el enfoque de la norma ISO 22301:2012. SIGNOS - Investigación En Sistemas de Gestión, 8(1), art. 31, 2017. DOI: https://doi.org/10.15332/s2145-1389.2016.0001.02
[32] Uche-M.M., Lucienne A., and Oghenevovwero-Zion. A.A., Conceptual Design of a Cybersecurity Resilience Maturity Measurement (CRMM) framework. The African Journal of Information and Communication (AJIC), 23, 2019. DOI: https://doi.org/10.23962/10539/27535
[33] Irene-Christine, D., and Thinyane, M., Comparative analysis of cyber resilience strategy in Asia-Pacific countries. 2020 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), 2020. DOI: https://doi.org/10.1109/dasc-picom-cbdcom-cyberscitech49142.2020.00027
[34] Chaudhary, M., and Chopra, A., Planning CMMI Implementation. CMMI for Development, pp 71-80, 2016. DOI: https://doi.org/10.1007/978-1-4842-2529-5_3
[35] Carrizo, D. y Alfaro, A., Método de aseguramiento de la calidad en una metodología de desarrollo de software: un enfoque práctico. Ingeniare. Revista Chilena de Ingeniería, 26(1), pp. 114-129, 2018. DOI: https://doi.org/10.4067/s0718-33052018000100114
[36] Combining NIST SP 800-55 and SP 800-26. Official (ISC)2® Guide to the ISSEP® CBK®, Second Edition, 2005, pp. 781-786. DOI: https://doi.org/10.1201/9780203888933.axc
[37] CANSO, Standard of excellence in cybersecurity, Civil Air Navigation Services Organization, [online]. 2020. [consultation, May 7, 2023]. Available at: https://canso.org/publication/canso-standard-of-excellence-in-cybersecurity/
[38] Meza, J.A.D., Castro, M.L.C., Vivas, R.V.J., and Rueda, A.C.C., Collaborative learning tools used in virtual higher education programs: a sistematic review of literature in Iberoamerica. In: 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020. DOI: https://doi.org/10.23919/cisti49556.2020.9140901
[39] Yogarajah, T., Shanmuganathan, V., and Kuhaneswaran, B., Evaluation and validation using Delphi method & field test for subfertility decision support system. 2020 From Innovation to Impact (FITI), 2020. DOI: https://doi.org/10.1109/fiti52050.2020.9424878
[40] Fajardo-Castro, L.V., Evaluación, diagnóstico e intervención: equipos de alto desempeño. Evaluación, Diagnóstico e Intervención En Psicología Organizacional: Nivel Grupo, pp 41-63, 2021. DOI: https://doi.org/10.14718/9789585133785.2021.3
[41] ISO 27001 and the management system requirements, ISO/IEC 27001:2022, 2022, pp 17-21. DOI: https://doi.org/10.2307/j.ctv30qq13d.6
[42] Bartock, M., Brule, J., Li-Baboud, Y.-S., Lightman, S., McCarthy, J., Reczek, K., Northrip, D., Scholz, A., and Suloway, T., Cybersecurity profile for the responsible use of Positioning, Navigation and Timing (PNT) services, 2020. DOI: https://doi.org/10.6028/nist.ir.8323-draft
[43] Amiruddin, A., Afiansyah, H.G., and Nugroho, H.A., Cyber-Risk management planning using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2021. DOI: https://doi.org/10.1109/icimcis53775.2021.9699337
[44] Bashofi, I., and Salman, M., Cybersecurity Maturity assessment design using NISTCSF, CIS CONTROLS v8 and ISO/IEC 27002. 2022 IEEE International Conference on Cybernetics and Computational Intelligence (CyberneticsCom), 2022. DOI: https://doi.org/10.1109/cyberneticscom55287.2022.9865640
[45] GCSCC, Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Ed. SSRN Electronic Journal, 2021. DOI: https://doi.org/10.2139/ssrn.3822153
[46] U.S. Departamento de Energía, Modelo de madurez de la capacidad de ciberseguridad (C2M2) versión 2.1, Departamento de Energía de EE.UU., Washington, DC, [online]. 2022. [consultation, May 7, 2023]. Available at: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf
[47] Amiruddin, A., Afiansyah, H.G., and Nugroho, H.A., Cyber-Risk management planning using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2021. DOI: https://doi.org/10.1109/icimcis53775.2021.9699337
[48] Dammert, D.L. y Núñez, L.C., Enfrentando las ciberamenazas: estrategias nacionales de ciberseguridad en el Cono Sur. Seguridad, Ciencia & Defensa, 5(5), pp. 107-129, [online]. 2019. [consultation, May 7th, 2023]. Available at: https://repositorio.utdt.edu/handle/20.500.13098/2294
[49] Herrera-Masó, J.R., Calero-Ricardo, J.L., González-Rangel, M.Á., Collazo-Ramos, M.I. y Travieso-González, Y., El método de consulta a expertos en tres niveles de validación. Revista Habanera de Ciencias Médicas, 21(1), [online]. 2022. [consultation, May 7th, 2023]. Available at: https://scielo.sld.cu/scielo.php?pid=S1729-519X2022000100014&script=sci_arttext&tlng=en
[50] CANSO, Standard of excellence in cybersecurity, Civil Air Navigation Services Organization, [online]. 2020. [consultation, May 7th, 2023]. Available at: https://canso.org/publication/canso-standard-of-excellence-in-cybersecurity/
[51] Visitsilp, B., and Bhumpenpein, N., Guidelines for Information technology governance based on integrated ISO 38500 and COBIT 2019. In: 2021 Research, Invention, and Innovation Congress: Innovation Electricals and Electronics (RI2C), 2021. DOI: https://doi.org/10.1109/ri2c51727.2021.9559772
[52] Zwarts, H., Du Toit, J., and Von Solms, B., A Cyber-Diplomacy and Cybersecurity Awareness Framework (CDAF) for developing countries. European Conference on Cyber Warfare and Security, 21(1), pp. 341-349, 2022. DOI: https://doi.org/10.34190/eccws.21.1.226
[53] Livshitz, I.I., Lontsikh, P.A., Lontsikh, N.P., Golovina, E.Y., and Safonova, O.M., The effects of cyber-security risks on added value of consulting services for IT-security management systems in holding companies. 2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS), 2020. DOI: https://doi.org/10.1109/itqmis51053.2020.9322883
[54] Neira-Melendrez, J.R., Seguridad de información en IoT y Big Data: un mapeo sistemático, [en línea]. 2021. [consulta, Mayo 7, 2023]. Disponible en: https://dspace.ups.edu.ec/bitstream/123456789/20578/1/UPS-GT003303.pdf
[55] Fernández-González, F.C., Fuentes-García-Romero-de-Tejada, C., González-Manzano, L. y Fuentes-García-Romero-de-Tejada, J.M.D., Revisión sistemática de la jurisprudencia española sobre ciberseguridad y privacidad (1995-2020), Revista de privacidad y derecho digital, VI (4), [en línea]. 2021. [consulta, Mayo 7, 2023]. Disponible en: https://e-archivo.uc3m.es/bitstream/handle/10016/34078/revision_RPDD_2021.pdf
[56] Tasheva, I., Cybersecurity post-COVID-19: lessons learned and policy recommendations. European View, 20(2), pp. 140-149, 2021. https://doi.org/10.1177/17816858211059250
[57] Perales-Manrique, J.H. y Molina-Chirinos, J.A., Modelo de madurez de analítica de datos para el sector financiero, 2020. DOI: https://doi.org/10.19083/tesis/652126
[58] Campos, J.L.S., Vigencia ontológica de la ciberseguridad en el marco de la seguridad informática chilena. Convenio de Budapest. Aula Virtual, 3(6), pp. 132-148, [en línea]. 2022. [consulta, Mayo 7, 2023].

Disponible en: https://hdl.handle.net/10983/30286
[59] Guayara-Murillo, E.A. y Moyano-Murcia, E.F., Propuesta de orientación en ciberseguridad para la formación de los estudiantes de media técnica especializada del colegio OEA IED basado en el marco NIST SP800-181, 2022. [consultation, May 7, 2023]. Available at: https://hdl.handle.net/10983/30286
[60] Armenta, E.R., and Carrillo, A.L.I. Towards an implementation of Information Technologies Governance. In: 2022 IEEE Mexican International Conference on Computer Science (ENC), 2022. DOI: https://doi.org/10.1109/enc56672.2022.9882923
[61] Pérez-Cuestas. J.A., Estrategia de capacitación en seguridad de la información basado en NIST 800-50 para una empresa en el sector financiero, 2022. [consultation, May 7, 2023]. Available at: https://hdl.handle.net/10983/27647
[62] Ebert, J., Newton, O., O'Rear, J., Riley, S., Park, J., and Gupta, M., Leveraging aviation risk models to combat cybersecurity threats in vehicular networks. Information, 12(10), 390, 2021. DOI: https://doi.org/10.3390/info12100390
[63] Ballestero, F., Cómo mejorar la ciberseguridad en España. Boletín Económico de ICE, 3148, 2022. DOI: https://doi.org/10.32796/bice.2022.3148.7457
[64] Mezher, A.A., and Mdlool, A.S., Relationship between continuous improvement and quality cybersecurity. PalArch's Journal of Archaeology of Egypt/Egyptology, 19(2), pp. 365-377, 2022. [consultation, May 7, 2023]. Available at: https://archives.palarch.nl/index.php/jae/article/view/11036
[65] Koza, E., Semantic analysis of ISO/IEC 27000 standard series and NIST cybersecurity framework to outline differences and consistencies in the context of operational and strategic information security. Med. Eng. Themes, 2, pp. 26-39, 2022. [consultation, May 7, 2023]. Available at: https://themedicon.com/pdf/engineeringthemes/MCET-02-021.pdf
[66] Hastings, N.A.J., ISO 55000 Series Standards. Physical Asset Management, pp. 595-621, 2021. DOI: https://doi.org/10.1007/978-3-030-62836-9_29
[67] Alsyouf, I., Alsuwaidi, M., Hamdan, S., and Shamsuzzaman, M., Impact of ISO 55000 on organisational performance: evidence from certified UAE firms. Total Quality Management & Business Excellence, 32(1-2), pp. 134-152, 2018. DOI: https://doi.org/10.1080/14783363.2018.1537750
[68] Ali, H., The strategic implementation asset management system basis ISO 55000: a case study on Indonesian Railways Company. Journal of Business Management Review, 2(3), pp. 226-244, 2021. DOI: https://doi.org/10.47153/jbmr23.1022021
[69] da-Silva, R.F., and de Souza, G.F.M., Modeling a maintenance management framework for asset management based on ISO 55000 series guidelines. Journal of Quality in Maintenance Engineering, 28(4), pp. 915-937, 2021. DOI: https://doi.org/10.1108/jqme-08-2020-0082
[70] Villanueva, G.A., Naranjo, A.F., and Jerez-Romero, E., Propuesta de mejora de la gestión de mantenimiento de los activos de una compañía certificadoras de productos y servicios, 2021. [consultation, May 7, 2023]. Available at: https://repositorio.ecci.edu.co/handle/001/1025
[71] -Cádiz, L.A., Sistema de información para la administración de activos fijos del Colegio María Inmaculada. Dr. Thesis, Universidad Andrés Bello, Santiago, Chile 2021. [consultation, May 7, 2023]. Available at: https://repositorio.unab.cl/xmlui/handle/ria/19233
[72] Angulo-Morris, M.A., Maceto-Rodríguez, J.F. y Quintana-Carbal, Y.F., Evaluación bajo la normatividad ISO 55000 de la gestión de activos al área de molienda de la empresa del sector minero de materiales preciosos Touchstone Colombia. 2022. [consultation, May 7, 2023]. Available at: https://bibliotecadigital.udea.edu.co/handle/10495/29982
[73] Parra, C., Viveros, P., Kristjanpoller, F., Crespo, A., González-Prida, V. y Gómez, J., Técnicas de auditorías para los procesos de: mantenimiento, fiabilidad operacional y gestión de activos (AMORMS & AMS-ISO 55001). INGEMAN, Escuela Superior de Ingenieros Industriales, Sevilla, España, 2 (35842.61124), 4, 2021. DOI: https://doi.org/10.13140/RG
[74] Torres-Martinez. A.M., Método de gestión de mantenimiento basado en la norma ISO 55000 para mejorar los indicadores de mantenimiento (RAM), en equipos de perforación de la Compañía Minera Las Bambas Arequipa-Perú 2021, 2021. [consultation, May 7, 2023]. Available at: https://www.researchgate.net/profile/Carlos-Parra-19/publication/349505815_TECNICAS_DE_AUDITORIA_PARA_LOS_PROCESOS_DE_MANTENIMIENTO_FIABILIDAD_OPERACIONAL_Y_GESTION_DE_ACTIVOS_AMORMS_AMS-ISO_55001/links/603efb2d92851c077f129ca6/TECNICAS-DE-AUDITORIA-PARA-LOS-PROCESOS-DE-MANTENIMIENTO-FIABILIDAD-OPERACIONAL-Y-GESTION-DE-ACTIVOS-AMORMS-AMS-ISO-55001.pdf
[75] Rodríguez-Ramos, P.A., Moreira-Mendoza, N.R. y Arteaga-Linzan, Á., Herramienta para la toma de decisiones en el reemplazo de activos. Ingeniería Mecánica, 25(1), pp. 1-7, 2022. [consultation, May 7, 2023]. Available at: https://scielo.sld.cu/scielo.php?pid=S1815-59442022000100001&script=sci_arttext&tlng=pt
[76] Putra, I.M.M., and Mutijarsa, K., Designing information security risk management on Bali Regional Police Command Center based on ISO 27005. In: 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT), 2021. DOI: https://doi.org/10.1109/eiconcit50028.2021.9431865 .
[77] Amiruddin, A., Afiansyah, H.G., and Nugroho, H.A., Cyber-Risk management planning using NIST CSF v1.1, NIST SP 800-53 Rev. 5, and CIS Controls v8. In: 2021 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), 2021. DOI: https://doi.org/10.1109/icimcis53775.2021.9699337
[78] Majid, S.A., Nugraha, A., Sulistiyono, B.B., Suryaningsih, L., Widodo, S., Kholdun, A.I., Febrian, W.D., Wahdiniawati, S.A., Marlita, D., Wiwah, A., and Endri, E., The effect of safety risk management and airport personnel competency on aviation safety performance. Uncertain Supply Chain Management, 10(4), pp. 1509-1522, 2022. DOI: https://doi.org/10.5267/j.uscm.2022.6.004
[79] Ullah, F., Qayyum, S., Thaheem, M.J., Al-Turjman, F., and Sepasgozar, S.M.E., Risk management in sustainable smart cities governance: a TOE framework. Technological Forecasting and Social Change, 167, art. 120743, 2021. DOI: https://doi.org/10.1016/j.techfore.2021.120743
[80] Luqman, A., Akram, M., and Alcantud, J.C.R., Digraph and matrix approach for risk evaluations under Pythagorean fuzzy information. Expert Systems with Applications, 170, art. 114518, 2021. https://doi.org/10.1016/j.eswa.2020.114518
[81] Angelopoulos, A.N., Bates, S., Candès, E.J., Jordan, M.I., and Lei, L.J., Learn then test: calibrating predictive algorithms to achieve risk control, 2021.
[82] Chow, Y.-L., and Pavone, M., A framework for time-consistent, risk-averse model predictive control: theory and algorithms. In: 2014 American Control Conference, 2014. DOI: https://doi.org/10.1109/acc.2014.6859437
[83] Khan, A., and Malaika, M., Central Bank risk management, fintech, and cybersecurity. SSRN Electronic Journal, 2021(105), 2021. DOI: https://doi.org/10.2139/ssrn.4026279
[84] Viktoriia, H., Hnatienko, H., and Babenko, T., An intelligent model to assess information systems security level. In: 2021 Fifth World Conference on Smart Trends in Systems Security and Sustainability (WorldS4), 2021. DOI: https://doi.org/10.1109/worlds451998.2021.9514019
[85] Almaiah, M.A., Al-Zahrani, A., Almomani, O., and Alhwaitat, A.K., Classification of cyber security threats on mobile devices and applications. Artificial Intelligence and Blockchain for Future Cybersecurity Applications, Studies in Big Data, 90, pp. 107-123, 2021. DOI: https://doi.org/10.1007/978-3-030-74575-2_6
[86] Saki, A.A., Suresh, A., Topaloglu, R.O., and Ghosh, S., Split compilation for security of quantum circuits. In: 2021 IEEE/ACM International Conference On Computer Aided Design (ICCAD), 2021. DOI: https://doi.org/10.1109/iccad51958.2021.9643478
[87] Pavón-González, Y., Ortega-González, Y.C., Infante-Abreu, M.B. y Delgado-Fernández, M., Método para proyectar el conocimiento de tecnologías de la información pertinente a la Ingeniería Industrial. Revista Universidad y Sociedad, 13(6), pp. 10-21, 2021. [consultation, May 7, 2023]. Available at: https://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202021000600010
[88] Rawal, B.S., Manogaran, G., and Peter, A., Recovery strategies for

database. Cybersecurity and Identity Access Management, 2022, pp. 201-207. DOI: https://doi.org/10.1007/978-981-19-2658-7_16

[89] González-Rodríguez, J.C. y Acevedo-Navas, C., Aproximación al panorama actual de la protección de infraestructuras críticas en Colombia. Panorama en seguridad y defensa visto desde las instituciones de educación superior de las Fuerzas Armadas, 2021, pp. 11-24. DOI: https://doi.org/10.21830/9789585380226.01

[90] Martínez-Rincón. L.C., Diseño técnico estructurado de un centro de respuesta a incidentes cibernéticos. 2021 [consultation, May 7, 2023]. Available at: https://repository.unad.edu.co/handle/10596/48312

[91] Velandia-Sanchez. F., Capacidades técnicas, legales y de gestión para equipos Blueteam y Redteam, 2020. [consultation, May 7, 2023]. Available at: https://repository.unad.edu.co/handle/10596/48107

[92] Almanza J.A.R., and Cano M.J.J., Cadenas de suministro. Revista Sistemas, 164, pp. 24-41, 2022. DOI: https://doi.org/10.29236/sistemas.n164a4

[93] Mariano-Díaz. R., Ciberseguridad en cadenas de suministros inteligentes en América Latina y el Caribe, 2022. [consultation, May 7, 2023]. Available at: https://repositorio.cepal.org/handle/11362/48065

[94] Valiente, J., (2022). Ciberseguridad en la cadena de suministro de la industria digital. Industria química, 99, pp. 57-59, 2022. [consultation, May 7, 2023]. Available at: https://dialnet.unirioja.es/servlet/articulo?codigo=8357825

[95] Miranda-Asuar, C., Gestión de riesgo de la cadena de suministro: un estudio de técnicas y herramientas. 2021. [consultation, May 7, 2023]. Available at: https://riunet.upv.es/handle/10251/175707

[96] Zamudio-Pereda, O., y Izquierdo-Requejo, A.A., Modelo de gestión de riesgo de la cadena de suministro como elemento diferenciador. Review of Global Management, 6(1), pp. 14-34, 2021. DOI: https://doi.org/10.19083/rgm.v6i1.1487

[97] Vega-de-la-Cruz, L.O., and Pérez-Pravia, M.C., Gestión integrada de riesgos de la seguridad de las cadenas de suministros con enfoque al servicio al cliente. Ingeniería y Competitividad, 24(02), art. 11197, 2022. DOI: https://doi.org/10.25100/iyc.v0i00.11197

[98] Sánchez Suárez, Y., Pérez Castañeira, J.A., Sangroni Laguardia, N., Cruz Blanco, C. and Medina-Nogueira, Y.E., Retos actuales de la logística y la cadena de suministro, 42(1), pp. 169-184, 2021. [consultation, May 7, 2023]. Available at: https://go.gale.com/ps/i.do?id=GALE%7CA678804788&sid=googleScholar&v=2.1&it=r&linkaccess=abs&issn=02585960&p=IFME&sw=w&userGroupName=anon%7E34d17fb5&aty=open+web+entry

[99] Pérez-Ramírez, R., Políticas, casos de estudio, técnicas de simulación y programas de competencias en la educación de logística y cadena de suministro en México, 2020, pp. 1-14. DOI: https://doi.org/10.35429/h.2020.1.1.14

[100] Castaño-Gómez, M., López-Echeverry, A.M., y Villa-Sánchez, P.A., Revisión del uso de tecnologías y dispositivos IoT en los sistemas de seguridad física. Ingeniería y Competitividad, 24(1), art. 11034, 2021. DOI: https://doi.org/10.25100/iyc.v24i1.11034

[101] Agyare, R., Adu-Boahene, C., y Nikoi, S.N., Gestión remota segura de redes y control de acceso a redes, el caso de la Universidad de Educación-Campus de Kumasi, 6(1), pp 18-45, 2021. DOI: https://doi.org/10.11648/j.ijse.20220601.13

[102] Collier, Z.A., and Sarkis, J., The zero trust supply chain: Managing supply chain risk in the absence of trust. International Journal of Production Research, 59(11), pp 3430-3445, 2021. DOI: https://doi.org/10.1080/00207543.2021.1884311

[103] Paredes, C.M., Martínez-Castro, D., Ibarra-Junquera, V., and González-Potes, A., Detection and isolation of DoS and Integrity cyber attacks in cyber-physical systems with a neural network-based architecture. Electronics, 10(18), art. 2238, 2021. DOI: https://doi.org/10.3390/electronics10182238

[104] Khader, M., Karam, M., and Fares, H., Cybersecurity awareness framework for academia. Information, 12(10), art. 417, 2021. DOI: https://doi.org/10.3390/info12100417

[105] Arblaster, M., 5 - Safety Regulation of Air Traffic Management. Air Traffic Management, pp. 87-115, 2018. DOI: https://doi.org/10.1016/b978-0-12-811118-5.00005-9

[106] Pollini, A., Callari, T.C., Tedeschi, A., Ruscio, D., Save, L., Chiarugi, F., and Guerri, D., Leveraging human factors in cybersecurity: an integrated methodological approach. Cognition, Technology & Work, 24(2), pp. 371-390, 2021. DOI: https://doi.org/10.1007/s10111-021-00683-y

[107] Bredenkamp, I.E., Kritzinger, E., and Herselman, M., A conceptual consumer data protection maturity model for government adoption: South African context. Lecture Notes in Networks and Systems, pp. 820-834, 2021. DOI: https://doi.org/10.1007/978-3-030-90318-3_64

[108] Rojas-Velásquez, R.G., y Muedas-Higginson, A.C., Modelo de madurez de seguridad de aplicaciones web ante ciberataques para clínicas de nivel 2, 2019 Available at: https://renati.sunedu.gob.pe/handle/sunedu/3003964

[109] Xie, Y., Gardi, A., and Sabatini, R., Cybersecurity trends in low-altitude air traffic management. in: 2022 IEEE/AIAA 41st Digital Avionics Systems Conference (DASC), 2022. DOI: https://doi.org/10.1109/dasc55683.2022.9925840

[110] Dolezilek, D., Gammel, D., and Fernandes, W., Cybersecurity based on IEC 62351 and IEC 62443 for IEC 61850 systems. 15th International Conference on Developments in Power System Protection (DPSP 2020), 2020. DOI: https://doi.org/10.1049/cp.2020.0016

[111] Bellini, E., Sargsyan, G., and Kavallieros, D., Cyber-resilience. Internet of Things, Threats, Landscape, and Countermeasures, pp. 291-333, 2021. DOI: https://doi.org/10.1201/9781003006152-8

[112] Martinez, S., Gransart, C., Stienne, O., Deniau, V., and Bon, P., SoREn, How dynamic software update tools can help cybersecurity systems to improve monitoring and actions. JUCS - Journal of Universal Computer Science, 28(1), pp 27-53, 2022. DOI: https://doi.org/10.3897/jucs.66857

[113] Li, Q., Li, Y., Liu, S., Wang, X., and Chaoui, H., Incomplete information stochastic game theoretic vulnerability management for wide-area damping control against cyber attacks. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 12(1), pp 124-134, 2022. DOI: https://doi.org/10.1109/jetcas.2022.3151645

[114] Sorge, C., IT Security measures and their relation to data protection. Law and Technology in a Global Digital Society, pp. 179-197, 2022. DOI: https://doi.org/10.1007/978-3-030-90513-2_10

[115] Kumar, R., and Venkatesh, K., Centralized and Decentralized data backup approaches. Advances in Intelligent Systems and Computing, pp. 687-698, 2022. DOI: https://doi.org/10.1007/978-981-16-5652-1_60

[116] Pérez-Sánchez, A., and Palacios, R., Evaluation of local security event management system vs. standard antivirus Software. Applied Sciences, 12(3), art. 1076, 2022. DOI: https://doi.org/10.3390/app12031076

[117] Zhang, X., Ma, H., and Tse, C.K., Assessing the robustness of cyber-physical power systems by considering wide-area protection functions. IEEE Journal on Emerging and Selected Topics in Circuits and Systems, 12(1), pp 107-114, 2022. DOI: https://doi.org/10.1109/jetcas.2022.3144443

[118] Potteiger, B., Dubey, A., Cai, F., Koutsoukos, X., and Zhang, Z., Moving target defense for the security and resilience of mixed time and event triggered cyber-physical systems. Journal of Systems Architecture, 125, art. 102420, 2022. DOI: https://doi.org/10.1016/j.sysarc.2022.102420

[119] Unal, U., Kahya, C.N., Kurtlutepe, Y., and Dag, H., Investigation of cyber situation awareness via SIEM tools: a constructive review. 2021 6th International Conference on Computer Science and Engineering (UBMK), 2021. DOI: https://doi.org/10.1109/ubmk52708.2021.9558964

[120] Laue, T., Kleiner, C., Detken, K.O., and Klecker, T., A SIEM architecture for multidimensional anomaly detection. 2021 11th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), 2021. DOI: https://doi.org/10.1109/idaacs53288.2021.9660903

[121] Bankole, F., Taiwo, A., and Claims, I., An extended digital forensic readiness and maturity model. Forensic Science International: Digital Investigation, 40, art. 301348, 2022. DOI: https://doi.org/10.1016/j.fsidi.2022.301348

[122] Folino, G., Godano, C.O., and Pisani, F.S., A scalable cybersecurity framework for anomaly detection in user behaviour, 2022. DOI: https://doi.org/10.21203/rs.3.rs-1912478/v1

[123] Sarker, I.H., Machine learning for intelligent data analysis and

automation in cybersecurity: current and future prospects, 2022. DOI: https://doi.org/10.20944/preprints202209.0032.v1

[124] Gómez-Orjuela, F.H., y Valencia-Valencia, H., Diseño de un procedimiento de gestión de incidentes de ciberseguridad que articule la gestión de riesgos, continuidad, crisis y resiliencia que se pueda integrar a la respuesta corporativa. 2021. DOI: https://doi.org/10.18235/0004373

[125] Senabre-López, S., Sota-Macia, I., y Munera-López, J., Fortaleciendo la ciberresiliencia del sector financiero. Revista de Estabilidad Financiera/Banco de España, pp 93-111, 2021. Available at: https://repositorio.bde.es/handle/123456789/19366

G. Brito-Acuña, is graduated as Electronic Technicianin 2004 and BSc. Eng in Computer Engineer in 2010, from the CUJAE. MSc. in Software Quality in the 4th edition of the University of Informatics Sciences. Since 2014, he has been a National Specialist in Aeronautical Cybersecurity at the Cuban Air Navigation Company and is a member of the global aeronautical cybersecurity working group. He has research interests in cybersecurity, risk management, aeronautics, resilience, operational security and the maturity of processes applied in critical CNS/ATM infrastructures.
ORCID: 0000-0003-0105-8178