Cybersecurity in Civil Aviation

Menotti Machado
Luiz Gustavo Cavallari

Cyber Security in Brazil

Brazil

- National Cyber Security Strategy – Decree 10.222/2020.
- National Law for Data Protection – Law 13.709/2018.
- National Network for Cyber Incidents Management – Decree 10.748/2021.

COM D CIBER

Army

SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA GABINETE DE

GSI

Cybernetic Guadian Exercise 4.0 (ComDCiber)

- Constructive Simulation
- Virtual Simulation (red team x blue team)
- Study Group – Air Transport Industry:
  - 2021: ISAC – Information Sharing and Analysis Center.
  - 2022: Study of a Framework to Audit Cybersecurity in Civil Aviation (UK-CAAi).

Cyber Security in ANAC

Regulation Responsibilities

- Air Space Control is an Air Force responsibility.

  - DECEA.

- ANAC is responsible to regulate: airports, air carriers, aircraft maintenance companies, aeronautical products companies, crew certification and passengers rights and duties.

Regulation

ANAC
AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

REGULAMENTO BRASILEIRO DA AVIAÇÃO CIVIL

RBAC nº 107

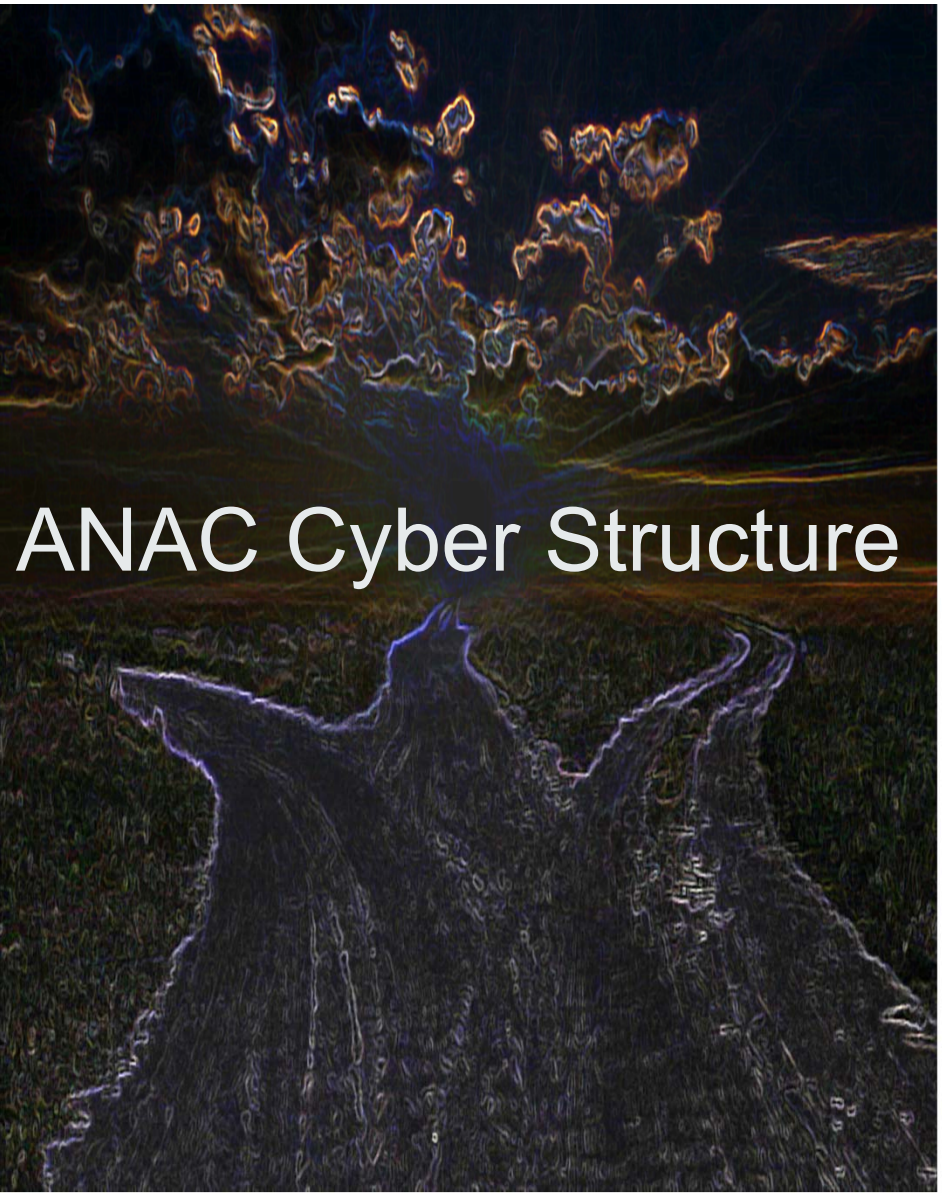
EMENDA nº 03

Título:	**SEGURANÇA DA AVIAÇÃO CIVIL CONTRA ATOS DE INTERFERÊNCIA ILÍCITA – OPERADOR DE AERÓDROMO**
Aprovação:	Resolução nº 362, de 16.07.2015. [Emenda nº 00] Resolução nº 385, de 09.08.2016. [Emenda nº 01] Resolução nº 500, de 12.12.2018. [Emenda nº 02] Resolução nº 604, de 29.01.2021. [Emenda nº 03]
Origem: SIA	

SUMÁRIO

- RBAC 108 EMD 03 – Aviation Security for Air Carriers:
  - 108.17(a) -The air operator must identify the information, data and communication technology systems deemed critical for its operation and implement measures to protect them, through a risk assessment.

- RBAC 107 EMD 03 – Aviation Security for Airport Operators:
  - 107.17(a) - The aerodrome operator shall design and implement an ongoing risk assessment process, with the objective of guiding airport security planning.



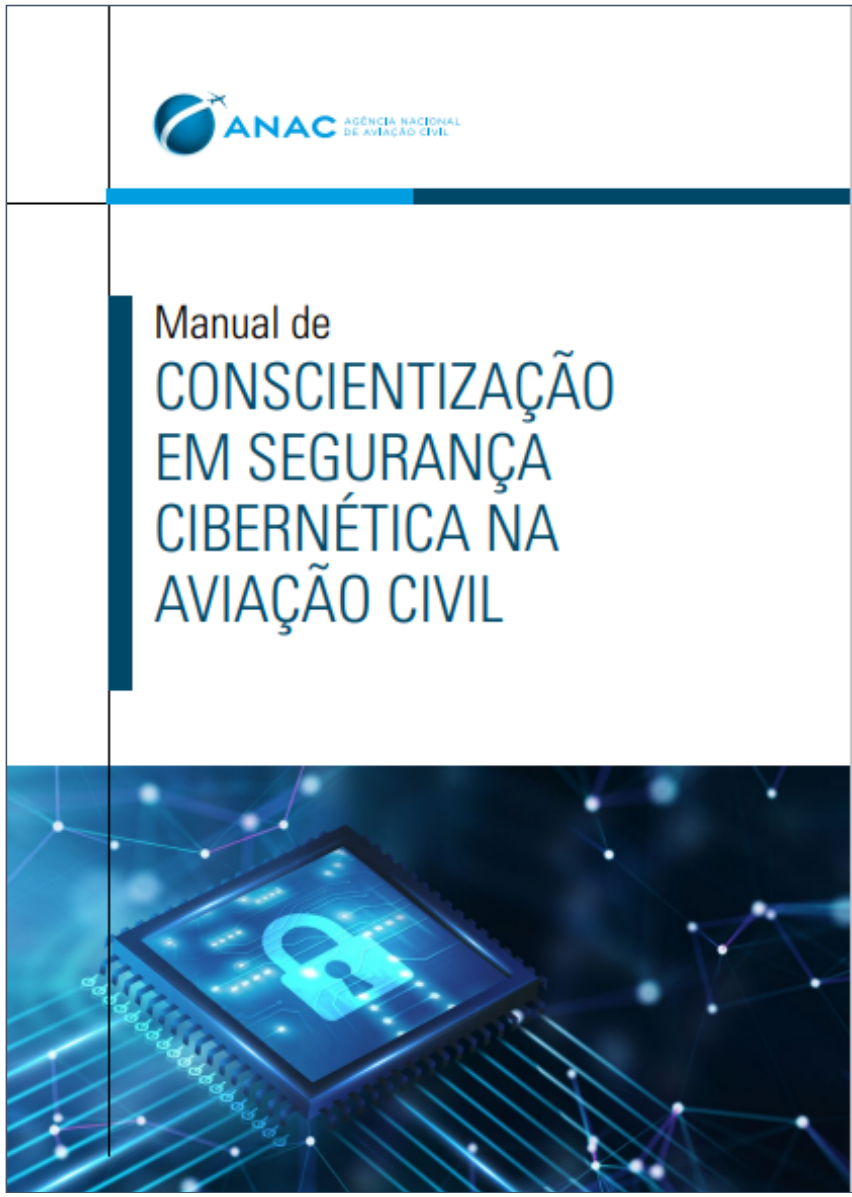
- Brazilian Aviation Security Team - BASeT (ICAO GASeP)
  - Working Group 4 of BASeT dedicated to cybersecurity;
  - Projects promoted by industry and government authorities.
- Data Protection and Information Security Committee (CSIP)
  - Internal focus at ANAC.
- GTSC (Work Group of Cybersecurity)
  - Dedicated to regulate cybersecurity for the ANAC attributions.

BASeT
Brazilian Aviation Security Team

Industry Participation

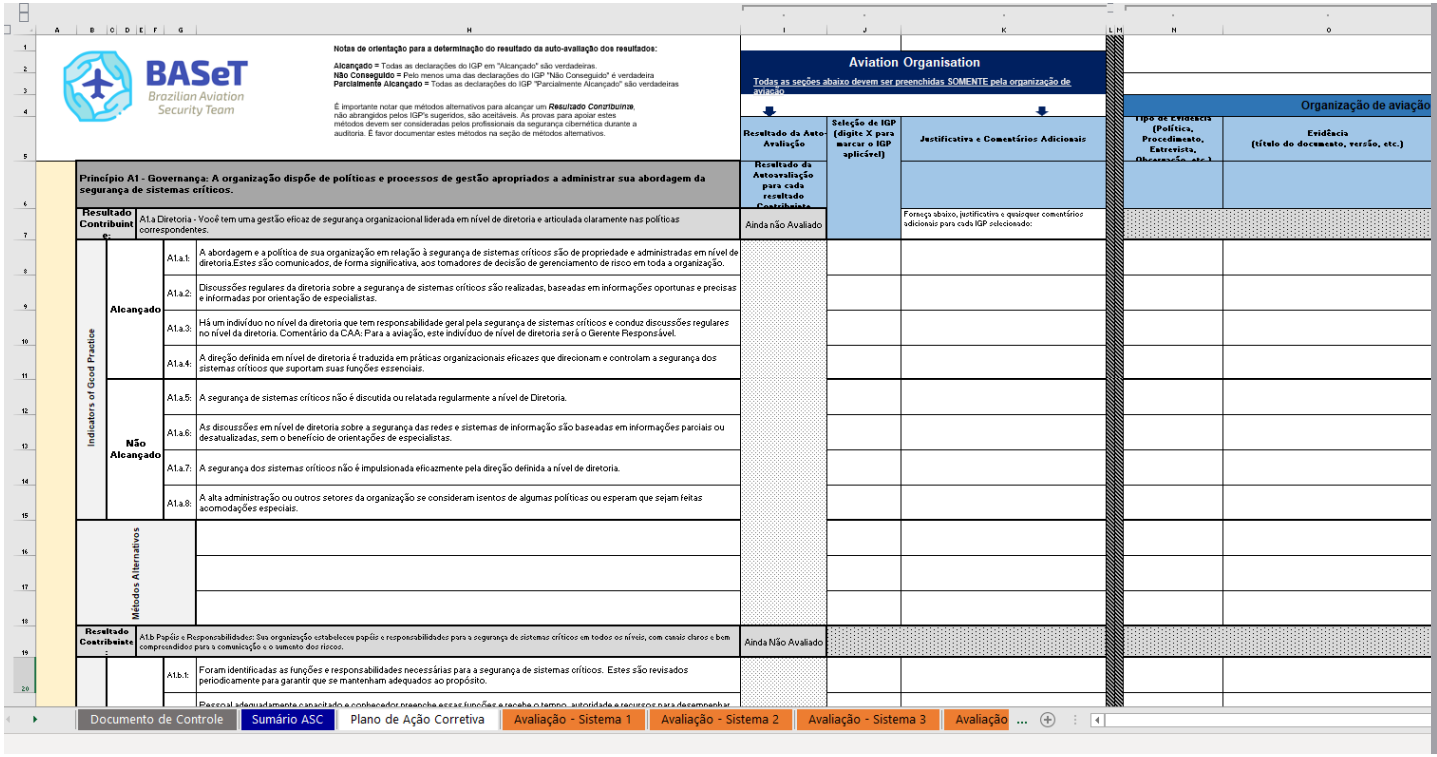
BASeT – Brazilian Aviation Security Team

- Working Group 4 – Cyber Security
  - Composed of Civil Aviation Authorities, associations and industry in general.
  - 2020/2021: Cyber Security Guidance Manual for Civil Aviation;
  - 2021/2022: Study of a Cyber Security Framework for Civil Aviation Organizations.



Study of a Cyber Security Framework for Civil Aviation Organizations.

BASeT
Brazilian Aviation Security Team



Notas de orientação para a determinação do resultado da auto-avaliação dos resultados:

Alcançado = Todas as declarações do IGP em "Alcançado" são verdadeiras.
Não Conseguido = Pelo menos uma das declarações do IGP "Não Conseguido" é verdadeira
Parcialmente Alcançado = Todas as declarações do IGP "Parcialmente Alcançado" são verdadeiras

É importante notar que métodos alternativos para alcançar um *Resultado Contribuinte*, não abrangidos pelos IGP's sugeridos, são aceitáveis. As provas para apoiar estes métodos devem ser consideradas pelos profissionais da segurança cibernética durante a auditoria. É favor documentar estes métodos na seção de métodos alternativos.

Aviation Organisation
Todas as seções abaixo devem ser preenchidas SOMENTE pela organização de aviação

Organização de aviação

			Resultado da Auto-Avaliação	Seleção de IGP (digite X para marcar o IGP aplicável)	Justificativa e Comentários Adicionais	Tipo de Evidência (Política, Procedimento, Entrevista, Observação, etc.)	Evidência (título do documento, versão, etc.)
Princípio A1 - Governança: A organização dispõe de políticas e processos de gestão apropriados a administrar sua abordagem da segurança de sistemas críticos.			Resultado da Autoavaliação para cada resultado Contribuinte				
Resultado Contribuinte:	A1.a Diretoria - Você tem uma gestão eficaz de segurança organizacional liderada em nível de diretoria e articulada claramente nas políticas correspondentes.		Ainda não Avaliado		Forneça abaixo, justificativa e quaisquer comentários adicionais para cada IGP selecionado:		
Indicators of Good Practice	**Alcançado**	A1.a.1: A abordagem e a política de sua organização em relação à segurança de sistemas críticos são de propriedade e administradas em nível de diretoria.Estes são comunicados, de forma significativa, aos tomadores de decisão de gerenciamento de risco em toda a organização.					
		A1.a.2: Discussões regulares da diretoria sobre a segurança de sistemas críticos são realizadas, baseadas em informações oportunas e precisas e informadas por orientação de especialistas.					
		A1.a.3: Há um indivíduo no nível da diretoria que tem responsabilidade geral pela segurança de sistemas críticos e conduz discussões regulares no nível da diretoria. Comentário da CAA: Para a aviação, este indivíduo de nível de diretoria será o Gerente Responsável.					
		A1.a.4: A direção definida em nível de diretoria é traduzida em práticas organizacionais eficazes que direcionam e controlam a segurança dos sistemas críticos que suportam suas funções essenciais.					
	Não Alcançado	A1.a.5: A segurança de sistemas críticos não é discutida ou relatada regularmente a nível de Diretoria.					
		A1.a.6: As discussões em nível de diretoria sobre a segurança das redes e sistemas de informação são baseadas em informações parciais ou desatualizadas, sem o benefício de orientações de especialistas.					
		A1.a.7: A segurança dos sistemas críticos não é impulsionada eficazmente pela direção definida a nível de diretoria.					
		A1.a.8: A alta administração ou outros setores da organização se consideram isentos de algumas políticas ou esperam que sejam feitas acomodações especiais.					
Métodos Alternativos							
Resultado Contribuinte:	A1.b Papéis e Responsabilidades: Sua organização estabelece papéis e responsabilidades para a segurança de sistemas críticos em todos os níveis, com canais claros e bem compreendidos para a comunicação e o aumento dos riscos.		Ainda Não Avaliado				
		A1.b.1: Foram identificadas as funções e responsabilidades necessárias para a segurança de sistemas críticos. Estes são revisados periodicamente para garantir que se mantenham adequados ao propósito.					
		Pessoal adequadamente capacitado e colaboradores preenche essas funções e recebe o tempo, autoridade e recursos para desempenhar					

Documento de Controle | Sumário ASC | Plano de Ação Corretiva | Avaliação - Sistema 1 | Avaliação - Sistema 2 | Avaliação - Sistema 3 | Avaliação ...

- Translated to portuguese the UK CAA Framework.
- Created a Guidance in portuguese to explain how to complete the Framework.
- Industry were fostered to use and give feedback.
- ANAC specialists are testing this framework with ANAC systems in order to analyse the use of this framework with the operators in the future.

ANAC' Internal Organization

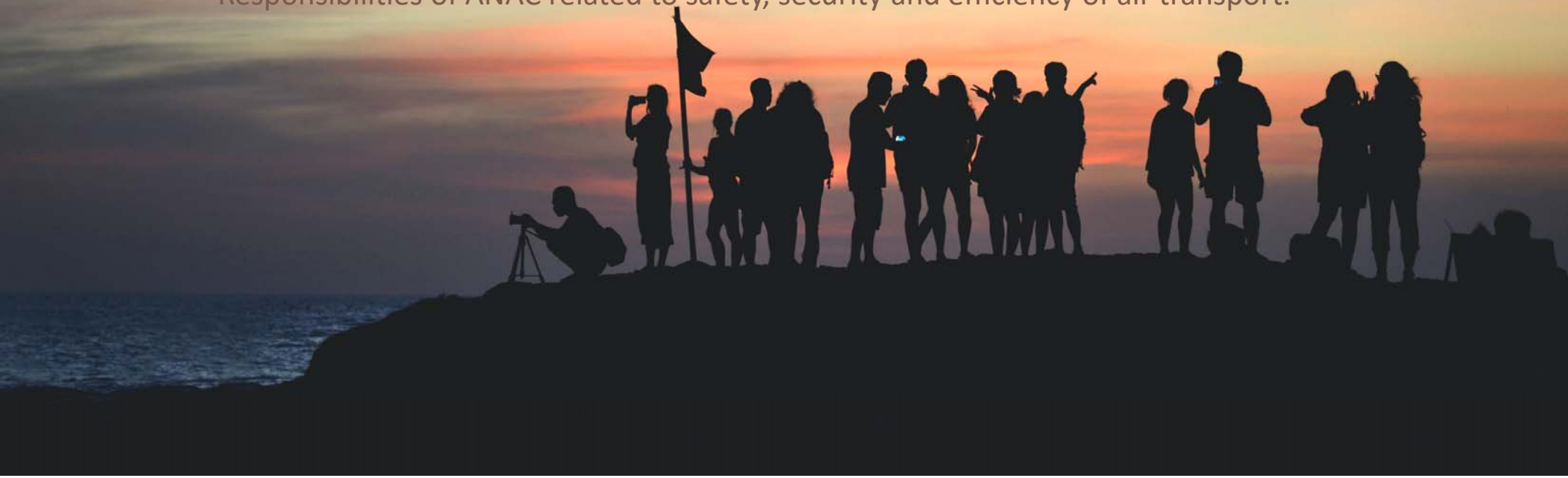
Data Protection and Information Security Committee (CSIP).

Formed by a group of ANAC employees responsible for proposing standards and supervision of information security and internal communications in ANAC.

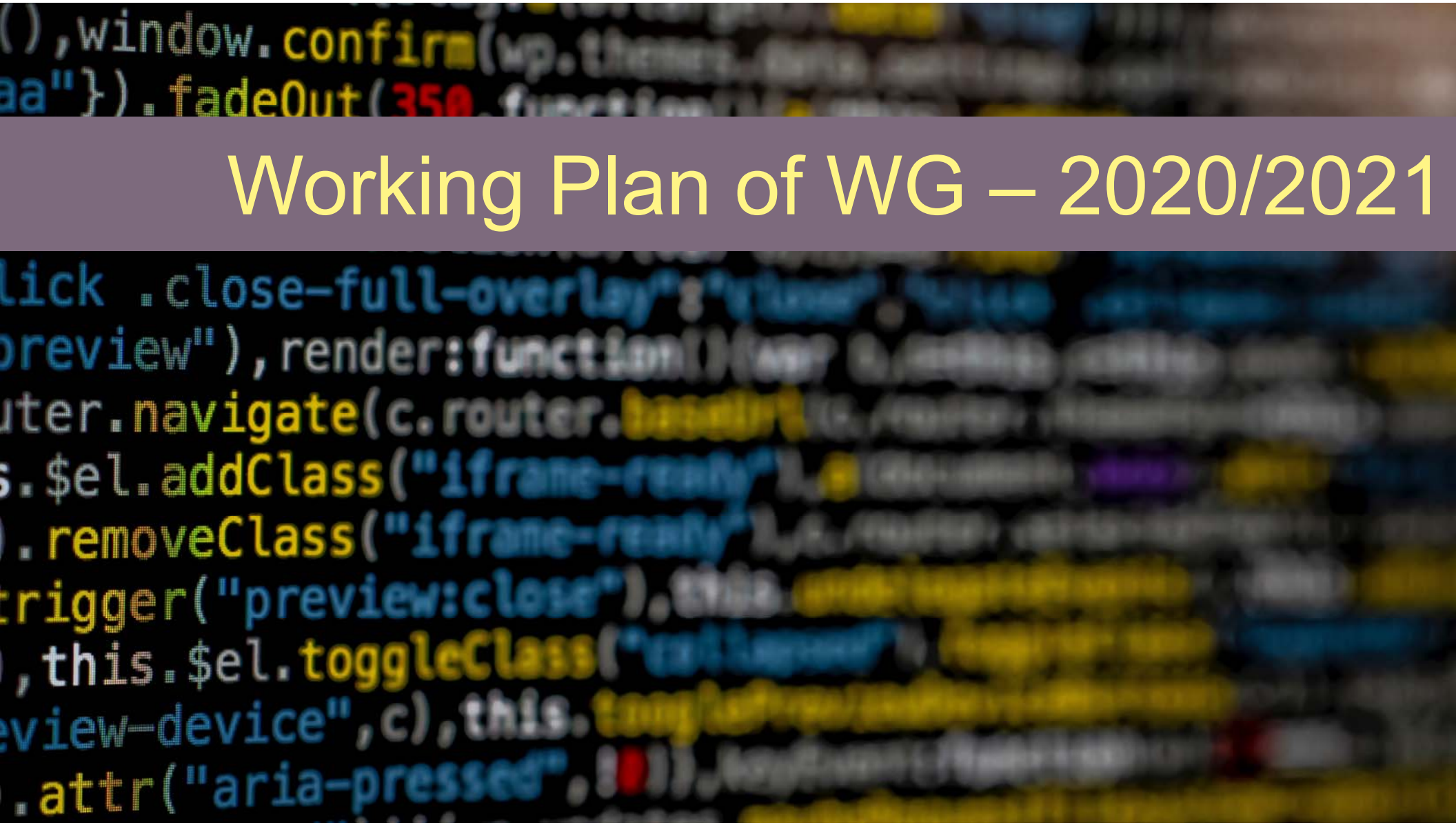

ANAC’ Working Group of Cyber Security

ANAC’ Working Group of Cyber Security

- Established on August 2020.
- Today: 22 members from 11 ANAC’ Organizational Units.
- Motivation:
  - Cyber technologies in air modal organizations;
  - Cyber threats with criminal or terrorist intent to cause damage to civil aviation;
  - Responsibilities of ANAC related to safety, security and efficiency of air transport.



ERICA JORDANA BENTO VIANA CRUZ
ANDERSON ANDRÉ OLIVEIRA DUARTE
RENATO HAMILTON SOUZA RODRIGUES
CLEUJANIO SILVA CRUZ
RODRIGO PIMENTA DE FIGUEIREDO
BERNARDO TOMAZ DE CASTRO
ROSEMBERG ANDRE DA SILVA
DIEGO PIVOTO PALMA
HENRIQUE TAITSON QUEIROZ
MENOTTI ERASMO DA SILVA MACHADO
LUIS GUSTAVO SILVA CAVALLARI
RICARDO ALBUQUERQUE DE OLIVEIRA
TÁRIK PEREIRA DE SOUZA
WERLLEN LAUTON ANDRADE
AUREO DE MORAIS VASCONCELOS
RICARDO NUNES
FELIPE SANTOS SARMANHO
REGINALDO LIRA DE ARAÚJO
FÁBIO OIKAWA DOS SANTOS
LEANDRO CRISPIM
MATEUS VIDAL ALVES SILVA



Working Plan of WG – 2020/2021

Working Plan

- 2020/2021:

1º Step: Diagnosis of Cyber Risk Scenarios in Civil Aviation

2º Step: Diagnosis about Cybernetics in each Unit of the Agency: Regulation, events and organizational structure.

3º Step: International Benchmarking.

4º Step: Analysis of Diagnosis and Benchmarking, with Suggestions for ANAC.


Step 1 – Risk Assessment

Cyber Risk Assessment Framework - Risk Matrix

Number	Risk Source: Technology and Database	Risk Scenarios	Impact	Probability	Existing regulation	ANAC Branch	Comments
14	Door lock system with keys through digital accreditation or biometrics.	Violation of the accreditation or door lock reading system.	Medium	Medium	RBAC107 107.93	SIA	
44	Equipment (tablet, cell phone, etc.) for passengers connected to the network provided by the aircraft	Intrusion by passenger equipment with subsequent theft or damage of data (loss of confidentiality and integrity), using the aircraft's system (entertainment).	Low	Very Low	-	SAR	
62	Calibration control system for the tools used by the maintenance organization	Loss of the calibration control system can impair the calibration of measurement and test equipment used to maintain the articles and periods which the equipment must be calibrated. Maintenance may be performed with uncalibrated equipment.	High	Medium	RBAC145.211 (C)(1)(viii)	SPO	
93	Ticket Sales and Customer Service Systems of Airlines	Unavailability of systems for a long time due to technical problems and/or hacker attack.	Medium	Medium	-	SAS	

Cyber Risks Assessment

Item	ANAC' Branch	Number of Scenarios (Total)	Number of Internal Scenarios	percentage of internal scenarios (%)	percentage of external scenarios (%)
1	SIA	40	4	10	90
2	SAR	31	18	58	42
3	SPO	47	3	6	94
4	SAS	10	1	10	90
5	SFI	12	12	100	0
6	SRA	9	9	100	0
7	ASSOP	5	1	20	80
8	SPL	9	7	78	22
9	all	163	55	34	66

Cyber Risks Assessment

Impact \ Probability	Very Low	Low	Medium	High	Very High
Very Low	2.4(%)	0.6(%)	1.2	0.0(%)	1.2(%)
Low	6.1(%)	3.1(%)	6.7(%)	0.0(%)	0.6(%)
Medium	6.1(%)	17.2(%)	8.6(%)	1.8(%)	1.2(%)
High	8.6(%)	12.9(%)	12.9(%)	0.0(%)	4.9(%)
Very High	0.6(%)	1.8(%)	0.6(%)	0.0(%)	0.0(%)

Step 2 – Internal Evaluation

ANAC Internal Diagnosis

Regulation
Events
Organizational structure
Training


Step 3 - Benchmarking

Benchmarking

- Websites research of various cybersecurity and aviation institutions.
- Relevant experiences identified, in particular:
  - United Kingdom CAA.
  - IATA.
  - EASA.
  - USA (TSA/FAA/CISA).

United Kingdom

- CAP 1753 – Cyber Security Oversight Process for Aviation
- CAP 1850 – Cyber Assessment Framework for Aviation (CAF)

IATA

Compilation of Cyber Security Regulations, Standards, and Guidance Applicable to Civil Aviation

TABLE 1. INTERNATIONAL INSTRUMENTS AND DOCUMENTS

Organization	Regulation / Standard / Recommendation Name	Purpose/Comments/Precis	Status	#Tag	Source (URL Link)
International Air Law Instruments	**Convention for the Suppression of Unlawful Seizure of Aircraft (1970)**	The **Hague Convention of 1970** was adopted in order to combat aircraft hijacking. It contains provisions for the criminalization of offences that are committed on board an aircraft in flight when a person seizes or exercises control of the aircraft. It needs to be noted that the Hague Convention may apply to aviation cyber security in case a passenger onboard takes control of the aircraft through a cyber-attack.	**In Force**	#Legal_Instrument #Convention #Aircraft	https://treaties.un.org/pages/showDetails.aspx?objid=0800000280112834
	Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)	The **Montreal Convention of 1971** takes an effect-based approach to determine the offences that have the following in common: the acts are unlawful and intentional, as well as the acts, are likely to endanger the safety of aircraft in flight. As per the provisions of the Montreal Convention and its applicability, there is no requirement for the offender to be on board an aircraft at the time of committing the unlawful act. Therefore, this broadens the applicability scope of the Montreal Convention and could include any remote cyber-attack affecting not only the aircraft but also air navigation facilities and any providers of critical information that are sent to the aircraft.	**In Force**	#Legal_Instrument #Convention #Transversal	https://www.un.org/ruleoflaw/blog/document/convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-civil-aviation/
	Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation, Supplementary to the Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation (1971)	The Montreal Convention was amended by the **Airport Protocol of 1988** with an aim to extend its catalog of offenses and include any unlawful acts (violence or disruption of services) at international airports. The scope of applicability relative to cyber-attacks is similar as introduced by the Montreal Convention of 1971; however, it is broadened to any cyber-attacks targeting the airport.	**In Force**	#Legal_Instrument #Convention #Aerodromes	https://www.un.org/ruleoflaw/blog/document/protocol-on-the-suppression-of-unlawful-acts-of-violence-at-airports-serving-international-civil-aviation-supplementary-to-the-convention-for-the-suppression-of-unlawful-acts-against-the-safety-of-civ/
	Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation (2010)	The **Beijing Convention of 2010** was introduced with the primary aim to consolidate the scope of the Montreal Convention of 1971 and the Airport Protocol of 1988. However, the Beijing Convention incorporated the broader jurisdiction bases, including the unlawful acts committed in the territory and/or national of that jurisdiction. The Beijing Convention further expands the applicability scope to the cyber-attacks targeting the air navigation facilities defining them as signals, data, information, or systems necessary for the aircraft navigation. Moreover, the Beijing Convention addresses any attacks on such facilities and aircraft conducted by cyber means.	**In Force**	#Legal_Instrument #Convention #Transversal	https://www.icao.int/secretariat/legal/Pages/TreatyCollection.aspx
	Beijing Supplementary Protocol to the 1970 Hague Convention for the Suppression of Unlawful Seizure of Aircraft (2010)	The **Beijing Supplementary Protocol of 2010** supplements the Hague Convention of 1970 and broadens the scope of unlawful acts reflecting the development and state of technology that may be used to commit unlaw[illegible] For the first time, the lega[illegible] within its scope	**In Force**	#Legal_Instrument #Convention #Aircraft	https://www.icao.int/secretariat/legal/Pages/TreatyCollection.aspx

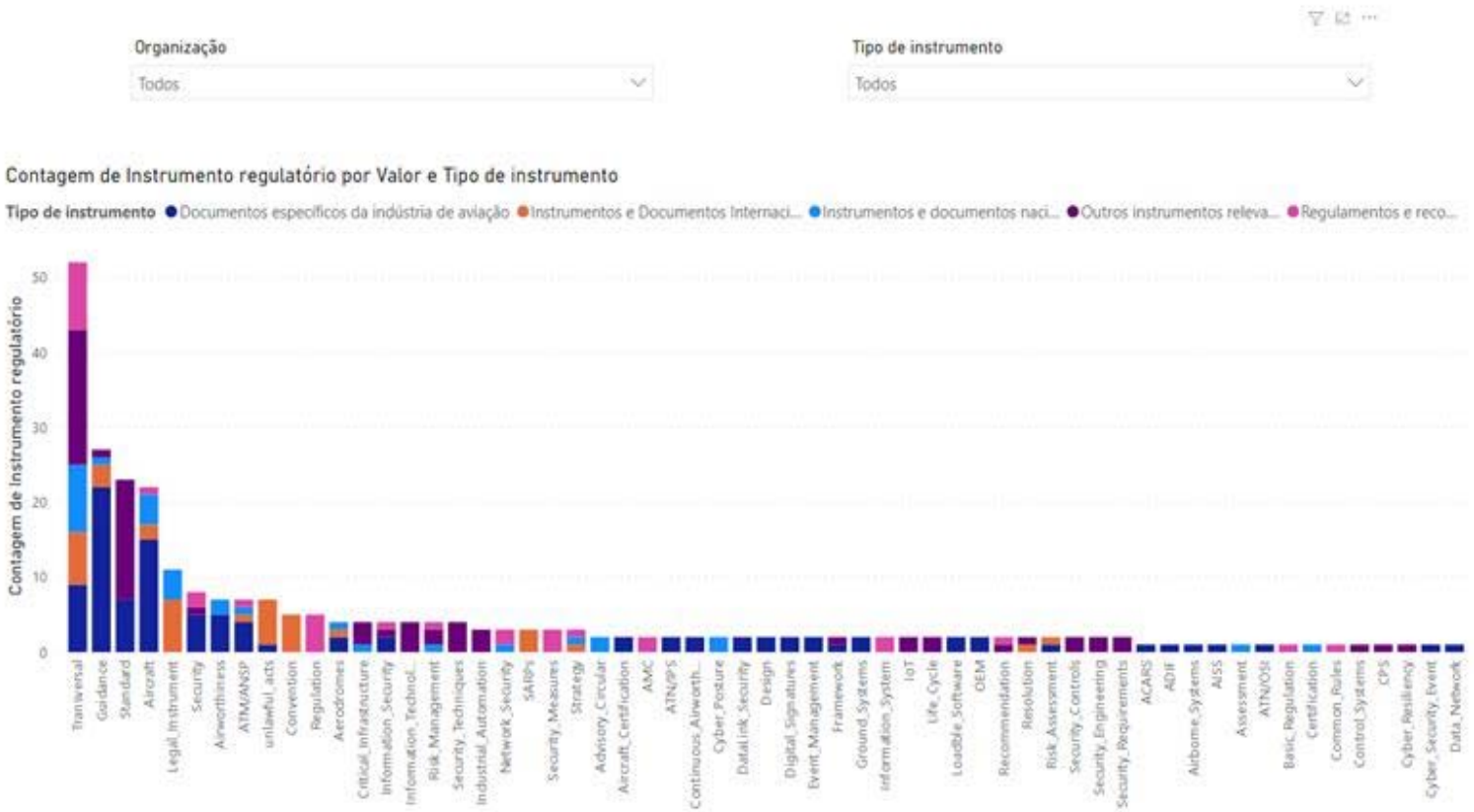
IATA

WG adapted the IATA compilation for Brazil through a “Power BI” solution.

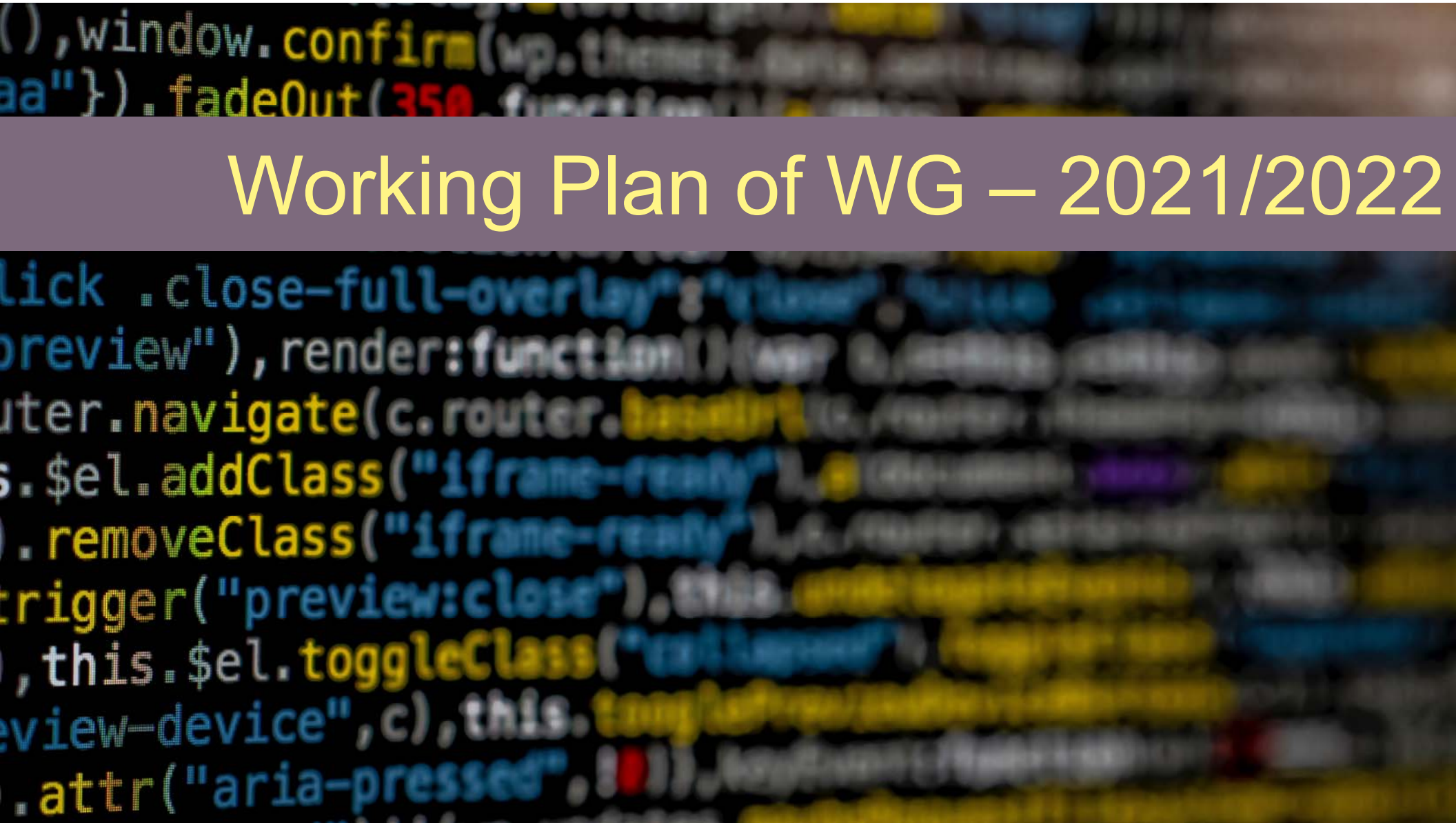
Organização	Instrumento regulatório	Resumo
A4A (Airline for America, former ATA)	ATA Spec 42 Aviation Industry Standards for Digital Information Security	Os padrões da indústria de aviação da ATA 42 para a segurança digital de segurança fornecem recomendações sobre métodos padronizados, a fim de obter um nível apropriado de segurança para os aplicativos que dependem de identidades digitais. Este documento visa fornecer orientação a uma variedade diferente de partes interessadas com requisitos de segurança.
Aeronautical Radio, Incorporated (ARINC)	ARINC Project Paper 858: Internet Protocol Suite (IPS) for Aeronautical Safety Services - Technical Requirements	O Papel de Projeto Arinc 858 é um documento com requisitos técnicos e padrões para sistemas ATN / IPS Airborne. ATN / IPS visa melhorar os serviços de comunicação de segurança da aviação.
Aeronautical Radio, Incorporated (ARINC)	ARINC Report 658 Internet Protocol Suite (IPS) for Aeronautical Safety Services - Roadmap Document	O Relatório de Arinc Report 658 Internet Protocol Suite (IPS) para serviços de segurança aeronáutica - Documento Roadmap fornece informações sobre a função de expansão da tecnologia de comunicação de dados, além de sua evolução, movendo-se de protocolos ACARS para ATN / OSI, e finalmente os protocolos ATN / IPS com redes. As normas relacionadas ao ATN / IPS são coordenadas com outras organizações de normas internacionais (isto é, ICAO, Eurocae e RTCA).
Aeronautical Radio, Incorporated (ARINC)	ARINC Report 811: Commercial Aircraft Information Security Concepts of Operation and Process Framework	O Relatório de Arinc 811: Os conceitos de segurança de informações comerciais da aeronave de operação e estrutura de processos fornecem informações para facilitar a compreensão da segurança das informações da aeronave, bem como para obter informações para ajudar o desenvolvimento de conceitos operacionais de segurança da informação da aeronave. O Relatório do Arinc 811 também fornece informações sobre a estrutura de processos de segurança da informação da aeronave para operadores de aeronaves de acordo com suas necessidades. Este documento, uma vez implementado, visa permitir o despacho seguro e seguro da aeronave a tempo. Além disso, a estrutura representa o desenvolvimento da segurança da informação da aeronave que é econômica, proporcionando também uma linguagem comum em termos de compreensão das necessidades de segurança.
Aeronautical Radio, Incorporated (ARINC)	ARINC Report 835-1 Guidance for Security of Loadble Software Parts Using Digital Signatures	O Relatório do Arinc 835-1 fornece informações técnicas de antecedentes e detalhadas em relação aos métodos existentes, a fim de proteger as peças de software carregáveis.
Aeronautical Radio, Incorporated (ARINC)	ARINC Report 852 Guidance for Security Event Logging in an IP Environment	O Relatório de Arinc 852 Orientação para o log de eventos de segurança em um ambiente IP fornece a orientação para redes e sistemas a bordo baseados em IP nos seguintes domínios de aeronaves: os Serviços de Informações Aéreas (AIS) e Informações de Passageiros e Serviços de Entretenimento (Tortas). O Relatório do Arinc 852 introduz um conjunto comum de elementos de dados relacionados à segurança e formato (s) produzidos (s) produzidos por sistemas de aeronaves.
Aeronautical Radio, Incorporated (ARINC)	ARINC Specification 664P1-2 Aircraft Data Network, Part 1, Systems Concepts and Overview	A rede de dados de aeronaves da especificação de Arinc 664P1-2, parte 1, conceitos de sistemas e visão geral fornece padrões sobre as redes de dados usadas em instalações comerciais de aeronaves. A especificação do Arinc 664P1-2 fornece informações sobre como adaptar os padrões de rede definidos comercialmente a um ambiente de aeronave.
Aeronautical Radio,	ARINC Specification 823P1 DataLink Security, Part 1 - ACARS	A ESPECIFICAÇÃO DA ARINC 823P1 DataLink Segurança, Parte 1 - A ACARS Message Security fornece padrões para a

IATA

WG adapted the IATA compilation for Brazil through a “Power BI” solution.




USA
ORDEM E PRO
- Cyber Security:
- Best Practicess;
- Responsabilities;
- Regulation;
- Oversight;
- Challenges.



Working Plan of WG – 2021/2022

Working Plan

- 2021/2022:

1º Step: Producing a Gap Analysis on the Application of the Decree that creates the National Network to Manage Cibernetic Incidents.

2º Step: Creation of a Cybersecurity Training Program at ANAC.

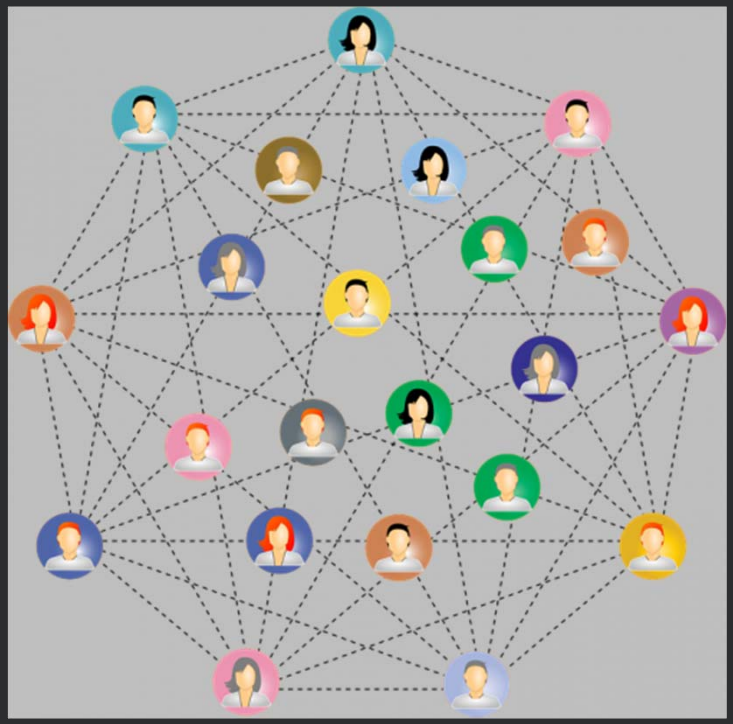
3º Step: Studying and monitoring of the ICAO Cybersecurity Strategy Action Plan (CyAP).

4º Step: Interaction with Subgroup 4 of BASeT (Filling of a Framework).

5° Step: Monitoring EASA Regulatory Developments.

1º - Federal Network to Manage Cibernetic Incidents

- As regulator, ANAC recieved new atributions to coordinate the cyber incidentes in Civil Aviation Industry.
- The Network:
  - National Information Security Department – CTIR Gov;
  - Setorial Coordenation Team - ANAC;
  - Main Teams - Operators Groups.
- This task is promoting a new cybersecurity structure at ANAC.



2º - Cybersecurity Training Program

- Research of a training programs:
  - Courses List.
    - Basic and advanced Cybernetics aspects of cyber security;
    - Cyber in Aviation;
    - Cybersecurity regulation;
    - National and foreign institutions.
  - Exchange knowledge and experience with other authorities and organizations.

Institution	Type	Course	Hours	Value

3º - Studying and Monitoring ICAO CyAP

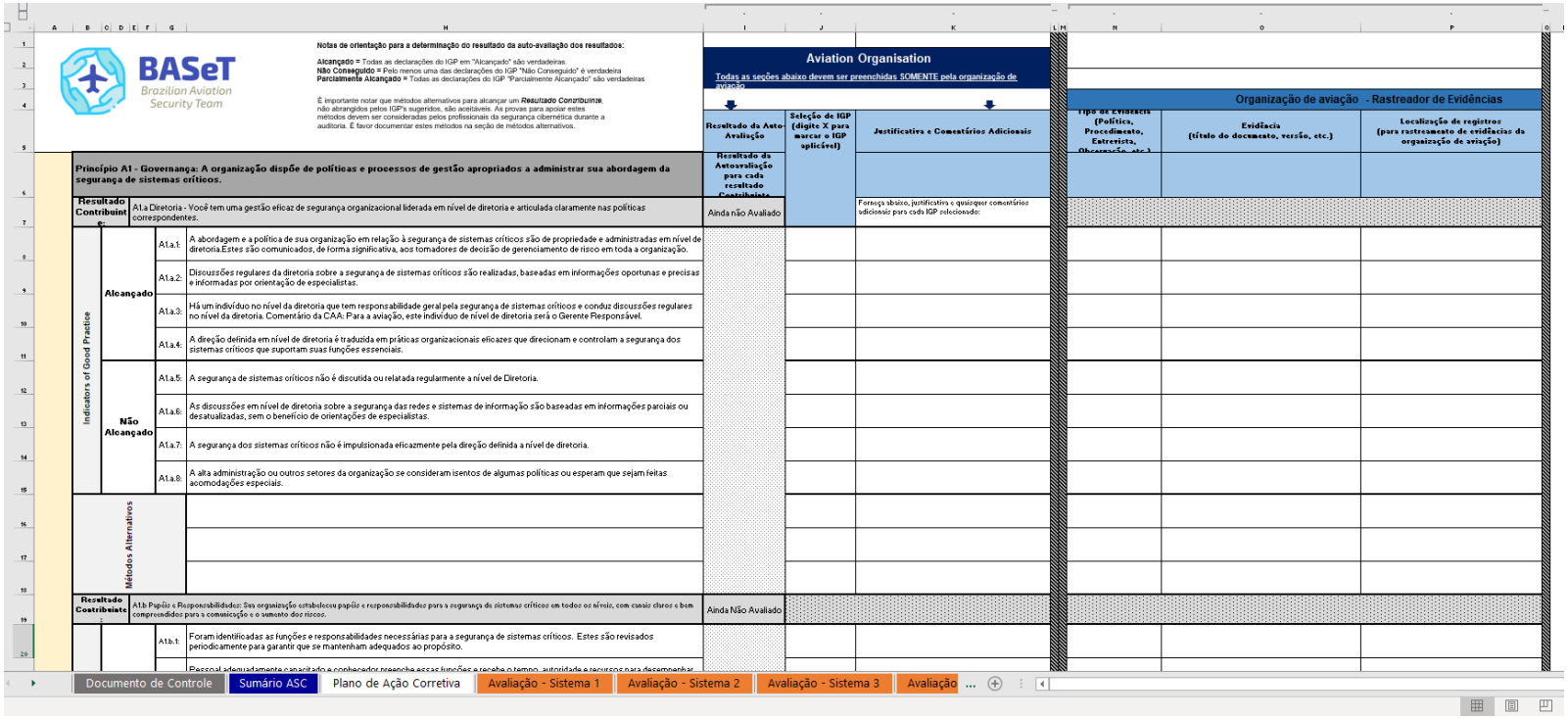
CYBERSECURITY ACTION PLAN - ROADMAP

								Ações					
ID	Pilar	Quem	ESC/PA	Medidas Específicas/Tarefas	Indicadores	Início	Palavras-chav	Atores no Brasil	Situação no Brasil	Ações no Brasil	Prioridades	Referências	Comentários
CyAP 3.1	Legislação Efetiva e Regulações	Estados Membros	ESC 3.3/PA 7.4	Estados-Membros devem ratificar os instrumentos da Convenção de Pequim.	Número de Estados que ratificaram os instrumentos da Convenção de Pequim.	Em curso	Supressão de atos ilícitos; Aviação civil internacional.	Presidência da República, Congresso Nacional	Em curso.	**Concluída**: Assinatura em 10/09/2010. **Pendente**: Ratificação.	Alta	https://www.icao.int/secretariat/legal/Lists/CurrentStatusOfPartiesAllItems.aspx https://www.icao.int/secretariat/legal/Status%20of%20Individual%20States/brazil_en.pdf	Verificar com ASINT se cabe alguma ação à ANAC neste contexto.
CyAP 3.2	Legislação Efetiva e Regulações	OACI	ESC 3.3/PA 7.3	Análise de instrumentos de direito aeronáutico internacional.	Revisão e análise de lacunas de instrumentos relevantes do direito aeronáutico internacional.	2022	Instrumentos; Direito aeronáutico internacional; Análise de Lacunas.	ANAC, DECEA, Autoridades Públicas Federais.	Não iniciada.	Aguardar propostas a serem apresentadas pelo secretariado da OACI nos fóruns adequados, para que o Brasil se manifeste e contribua.	Alta	https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10748.htm	**Legislação existente:** Decreto nº 10.222 de 05/02/2020 Aprova a Estratégia Nacional de Segurança Cibernética. Decreto nº 10.748 de 16/07/2021 Institui a Rede Federal de Gestão de Incidentes Cibernéticos.
CyAP 3.3	Legislação Efetiva e Regulações	OACI, Estados Membros	ESC {3.3; 3.4}/ PA 7.2	Análise da legislação nacional existente no campo da segurança cibernética da aviação civil e identificação de lacunas, inclusive no direito penal.	Levantamento sobre a situação da legislação nacional no que diz respeito ao enfrentamento de atos ilícitos contra a aviação civil cometidos por meios cibernéticos.	2023-2024	Legislação existente; Segurança cibernética; Atos ilícitos; Análise.	ANAC, DECEA, Autoridades Públicas Federais.	Não iniciada.	Aguardar propostas a serem apresentadas pelo secretariado da OACI nos fóruns adequados, para que o Brasil se manifeste e contribua.	Média	https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/d10222.htm https://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2021/Decreto/D10748.htm	**Legislação existente:** Decreto nº 10.222 de 05/02/2020 Aprova a Estratégia Nacional de Segurança Cibernética. Decreto nº 10.748 de 16/07/2021 Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Pesquisar propostas de lei no congresso. Contatar GSI para consulta sobre o assunto. Contatar TCU, PF. Consultar OACI para obter detalhes da ação.
CyAP 3.4	Legislação	OACI	ESC 3.3/PA 7.1	Revisão de padrões e práticas recomendadas da OACI existentes para	Revisão e análise de lacunas dos SARPs	2022	Padrões e práticas recomendadas; Segurança	ANAC, DECEA, Autoridades	Não iniciada	Aguardar propostas a serem apresentadas pelo secretariado da OACI nos fóruns	Alta		Uma vez apresentadas as propostas de alteração em SARPs, avaliar o impacto disto em leis/decretos e regulações em efeito no Brasil.

GASeP National | Plan1

4º Step: Interaction with Subgroup 4 of BASeT (Filling the Framework).

BASeT
Brazilian Aviation Security Team



Notas de orientação para a determinação do resultado da auto-avaliação dos resultados:

Alcançado = Todas as declarações do IGP em "Alcançado" são verdadeiras.
Não Conseguido = Pelo menos uma das declarações do IGP "Não Conseguido" é verdadeira
Parcialmente Alcançado = Todas as declarações do IGP "Parcialmente Alcançado" são verdadeiras

É importante notar que métodos alternativos para alcançar um **Resultado Contribuinte**, não abrangidos pelos IGP's sugeridos, são aceitáveis. As provas para apoiar estes métodos devem ser consideradas pelos profissionais da segurança cibernética durante a auditoria. É favor documentar estes métodos na seção de métodos alternativos.

Aviation Organisation
Todas as seções abaixo devem ser preenchidas SOMENTE pela organização de aviação

Organização de aviação - Rastreador de Evidências

			Resultado da Auto-Avaliação	Seleção de IGP (digite X para marcar o IGP aplicável)	Justificativa e Comentários Adicionais	Tipo de Evidência (Política, Procedimento, Entrevista, Observação, etc.)	Evidência (título do documento, versão, etc.)	Localização de registros (para rastreamento de evidências da organização de aviação)
Princípio A1 - Governança: A organização dispõe de políticas e processos de gestão apropriados a administrar sua abordagem da segurança de sistemas críticos.			Resultado da Autoavaliação para cada resultado Contribuinte					
Resultado Contribuinte:	A1.a Diretoria - Você tem uma gestão eficaz de segurança organizacional liderada em nível de diretoria e articulada claramente nas políticas correspondentes.		Ainda não Avaliado		Forneça abaixo, justificativa e quaisquer comentários adicionais para cada IGP selecionado:			
Indicators of Good Practice	**Alcançado**	A1.a.1:	A abordagem e a política de sua organização em relação à segurança de sistemas críticos são de propriedade e administradas em nível de diretoria.Estes são comunicados, de forma significativa, aos tomadores de decisão de gerenciamento de risco em toda a organização.					
		A1.a.2:	Discussões regulares da diretoria sobre a segurança de sistemas críticos são realizadas, baseadas em informações oportunas e precisas e informadas por orientação de especialistas.					
		A1.a.3:	Há um indivíduo no nível da diretoria que tem responsabilidade geral pela segurança de sistemas críticos e conduz discussões regulares no nível da diretoria. Comentário da CAA: Para a aviação, este indivíduo de nível de diretoria será o Gerente Responsável.					
		A1.a.4:	A direção definida em nível de diretoria é traduzida em práticas organizacionais eficazes que direcionam e controlam a segurança dos sistemas críticos que suportam suas funções essenciais.					
	Não Alcançado	A1.a.5:	A segurança de sistemas críticos não é discutida ou relatada regularmente a nível de Diretoria.					
		A1.a.6:	As discussões em nível de diretoria sobre a segurança das redes e sistemas de informação são baseadas em informações parciais ou desatualizadas, sem o benefício de orientações de especialistas.					
		A1.a.7:	A segurança dos sistemas críticos não é impulsionada eficazmente pela direção definida a nível de diretoria.					
		A1.a.8:	A alta administração ou outros setores da organização se consideram isentos de algumas políticas ou esperam que sejam feitas acomodações especiais.					
Métodos Alternativos								
Resultado Contribuinte:	A1.b Papéis e Responsabilidades: Sua organização estabeleceu papéis e responsabilidades para a segurança de sistemas críticos em todos os níveis, com canais claros e bem compreendidos para a comunicação e o aumento dos riscos.		Ainda Não Avaliado					
		A1.b.1:	Foram identificadas as funções e responsabilidades necessárias para a segurança de sistemas críticos. Estes são revisados periodicamente para garantir que se mantenham adequados ao propósito.					
			Pessoal adequadamente capacitado e conhecedor preenche essas funções e recebe o tempo, autoridade e recursos para desempenhar					

Documento de Controle | Sumário ASC | Plano de Ação Corretiva | Avaliação - Sistema 1 | Avaliação - Sistema 2 | Avaliação - Sistema 3 | Avaliação ...

5º - Monitoring EASA Regulatory Developments

- Specific regulations for aeronautical products.
- Wide regulation for other institutions:
  - (NPA 2019-07): Management of Information Security Risks (ISMS);
  - Similar to SMS/SeMS;
  - Based on ISO 27001.

EASA
European Aviation Safety Agency


Thank you!
Cyber Security Coordination - ANAC
ANAC