ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

BASeT Brazilian Aviation Security Team

Manual de USO DA AVALIAÇÃO DE SEGURANÇA CIBERNÉTICA (ASC) PARA A AVIAÇÃO

MANUAL DE USO DA AVALIAÇÃO DE SEGURANÇA CIBERNÉTICA

Fevereiro / **2023**

BASET - SUBGRUPO 4

MEMBROS	
Marcelo Pedroso	Ticianne Sanches da Silveira
Ana Carla Ramos de Lucena	Eduardo Seidenberger
Menotti Erasmo da Silva Machado	Nilo Arthur Ericsen Ferreira
Luiz Gustavo Silva Cavallari	Patricia Silva Patta
Rodrigo Pereira Damásio da Silva	Lenise Maria M Falcoski Soldan
Douglas Rebouças de Almeida	Eduardo Luiz Tarifa Pinto
Mariana Silveira de Menezes	Altair Zuolo Junior
Rodrigo Pires	Bruno Rodrigues Marques Valle
Adélcio Enéas Peres	Vilson Borges Bentien
Bernard Souza da Silva	Wilson Felicio Victer

PROJETO GRÁFICO E DIAGRAMAÇÃO

Assessoria de Comunicação Social (Ascom)

DÚVIDAS, SUGESTÕES E CRÍTICAS PODEM SER ENVIADAS PARA O E-MAIL

sia@anac.gov.br

SUMÁRIO

1. INTRODUÇÃO

Os riscos associados à segurança cibernética são dinâmicos, o que significa que os perpetradores estão sempre procurando explorar vulnerabilidades e podem desenvolver rapidamente novas maneiras de violar a segurança cibernética. Os sistemas progressivamente interconectados da indústria da aviação exigem que a indústria se dedique a uma consciência atualizada das ameaças diretas e indiretas à segurança cibernética. O cenário de ameaças em mudança, portanto, incentiva uma abordagem proativa à segurança cibernética e, em resposta, significa que as organizações de aviação precisam de proteção dinâmica.

A VISÃO SOBRE A AVALIAÇÃO DE SEGURANÇA CIBERNÉTICA É:

> *"Ter uma abordagem proporcional e eficaz para a avaliação que permita à aviação gerenciar seus riscos de segurança cibernética sem comprometer a security, safety ou resiliência da aviação.*
>
> *Buscando estabelecer padrões mínimos de atualização de forma a influenciar positivamente a segurança cibernética dentro da aviação para apoiar a Estratégia Nacional de Segurança Cibernética Brasil."*

Este documento fornece orientações sobre como completar a Avaliação de Segurança Cibernética (ASC) para Aviação.

2. CONTEXTO

O Grupo Brasileiro de Segurança da Aviação Civil contra Atos de Interferência Ilícita (*Brazilian Aviation Security Team* - BASeT) é um comitê sem personalidade jurídica, instituído pela Resolução nº 542, de 18 de fevereiro de 2020.

A Resolução/ANAC nº 542/2020 busca formalizar fórum de debates que, desde junho de 2018, vêm ocorrendo entre diversos atores envolvidos com a temática AVSEC (*Aviation Security*), cuja diretriz de planejamento dos trabalhos ocorre em consonância com o Plano Global de Segurança da Aviação Civil (GASeP - *Global Aviation Security Plan*), instituído pela Organização da Aviação Civil Internacional (OACI).

Entre os atores envolvidos estão operadores aéreos, operadores aeroportuários, entidades públicas como Departamento de Controle do Espaço Aéreo (DECEA), Departamento de Polícia Federal e instituições da comunidade de aviação civil dedicadas à melhoria da segurança da aviação civil brasileira, como ABEAR, IATA, ALTA, ANEAA.

A ASC foi proposta pelo Subgrupo 4 do BASeT como um dos produtos do Ciclo de Atividades 2021/20222. Ela consiste na criação de uma Estrutura de Avaliação de Segurança Cibernética para Organizações da Aviação Civil. Ela representa uma tradução, com algumas adaptações, do CAP 1850 (Guia da Estrutura de Avaliação Cibernética para a Aviação - *Cyber Assessment Framework* (CAF) for *Aviation Guidance*) publicado pela Autoridade da Aviação Civil do Reino Unido. Assim, a partir da análise da experiência empreendida pelo Reino Unido, ela foi adaptada para a realidade da aviação civil brasileira, de maneira a servir de suporte básico e de referencial ao monitoramento de segurança cibernética nestas organizações. Inclusive devendo atender, em especial, ao seguinte conjunto de requisitos:

- Fornecer uma estrutura adequada para auxiliar na realização de avaliações de resiliência cibernética na aviação civil;
- Manter a abordagem focada nos resultados dos princípios de segurança cibernética e resiliência e desencorajar avaliações que possam ser realizadas como exercícios de conformidade (*tick-box*);
- Ser compatível com o uso de orientações e normas adequadas de segurança cibernética existentes;
- Permitir a identificação de atividades eficazes de segurança cibernética e melhoria da resiliência;
- Ser extensível para acomodar elementos setoriais específicos, conforme necessário;
- Permitir a definição de níveis significativos de segurança para as organizações alcançarem, possivelmente que reflitam uma visão de segurança adequada e proporcional; e
- Ser o mais simples e econômico possível para aplicação.

2.1. VISÃO GERAL DA ASC

A ASC foi elaborada para fornecer uma avaliação focada em resultados que consideram quatorze princípios de quatro objetivos amplos. Os princípios são ainda divididos em trinta e nove Resultados Contribuintes. Cada resultado está associado a um conjunto de Indicadores de Boas Práticas (IGPs) que são divididos nas três categorias seguintes:

- A coluna '**Alcançado**' de uma tabela IGP define as características típicas de uma organização que alcança plenamente esse resultado. Pretende-se como meta que todos os indicadores estejam presentes para apoiar uma avaliação de 'Alcançado';
- A coluna '**Não Alcançado**' de uma tabela IGP define as características típicas de uma organização que não alcança esse objetivo por razões diversas a ser identificadas. Pretende-se que a presença de qualquer indicador leve a uma avaliação de "Não Alcançado"; e
- Quando presente, a coluna '**Parcialmente Alcançado**' de uma tabela IGP define as características típicas de uma organização que alcança parcialmente esse resultado.

Os resultados da aplicação da ASC para aviação são trinta e nove avaliações individuais, cada uma derivada de um julgamento sobre até que ponto um conjunto de IGPs reflete as circunstâncias da organização de aviação que está sendo avaliada. A ASC foi projetada de tal forma que um resultado no qual todos os trinta e nove Resultados Contribuintes foram avaliados como "Alcançados" indicaria um nível de segurança cibernética de alguma forma devido ao nível mínimo de "higiene cibernética básica".

A avaliação dos Resultados Contribuintes é principalmente uma questão de julgamento de especialistas e as tabelas do IGP não removem a exigência de expertise em segurança cibernética e de conhecimento da aviação civil. Os profissionais devem usar o resultado do trabalho para considerar a postura de segurança cibernética de uma organização ao lado do contexto do setor e quaisquer fatores relevantes adicionais.

2.2. NOTAS

Ao completar a ASC, as organizações de aviação civil devem ter em mente o seguinte:

- A ASC não se destina a ser exaustiva e não é em si um indicador de conformidade.
- A ASC não tem o objetivo de ser inflexível, baseada em regras ou aplicada como uma lista de verificação, sendo que quando um Indicador de Boas Práticas não está sendo cumprido, a organização de aviação deve buscar implementar na medida do possível controles alternativos ou métodos que atendam ao Resultado Contribuinte.
- Não se espera que todas as organizações de aviação civil marquem 'Alcançados' para cada Resultado Contribuinte.

3. PREENCHENDO A AVALIAÇÃO DE SEGURANÇA CIBERNÉTICA - ASC

A ASC consiste em guias-chave denominadas:

- Documento de Controle;
- Sumário ASC (Organização da Aviação);
- Plano de Ação Corretiva; e
- Avaliação – Sistema (1-25).

Todas as guias devem ser preenchidas usando as opções de drop-down fornecidas (quando aplicável) e caixas de texto.

3.1. DOCUMENTO DE CONTROLE

Esta guia contém informações incluindo; número da versão, informações de fundo e links para orientação referenciada.

3.2. SUMÁRIO ASC (ORGANIZAÇÃO DA AVIAÇÃO)

A guia "Sumário ASC (Organização da Aviação)" fornece à organização de aviação uma visão resumida de sua posição referenciada em cada um dos Resultados Contribuintes. Em grande parte, esta guia não requer nenhum preenchimento da organização de aviação, exceto complementar a tabela "Informações sobre a Organização" mostrada abaixo.

Informação Organizacional	
Empresa	
Gerente de Segurança Cibernética Responsável	
Número de Sistemas Críticos	1

Sumário ASC (Organização da Aviação)

NOTA:

Todos os gráficos e células de sistemas na guia resumo irão preencher automaticamente todo o Sumário a partir de cada guia "Avaliação".

4. AVALIAÇÃO – SISTEMA (1 – 25)

As guias de avaliação devem ser utilizadas por uma organização de aviação para concluir uma autoavaliação contra cada um dos Resultados Contribuintes para cada um dos sistemas críticos identificados.

A ASC gera até 25 guias de avaliação de sistemas separadas e, caso sejam necessárias guias adicionais, use uma nova pasta de trabalho da ASC. Quando algumas guias não se mostrarem necessárias, deixe-as em branco, caso contrário se os campos forem excluídos o resultado final não refletirá a informação esperada com precisão. A guia de resumo simplesmente mostrará isso como "ainda não avaliado".

NOTA:

Onde os Resultados Contribuintes são geralmente "organizacionais" (por exemplo, A1. Governança) estes devem ser preenchidos na íntegra na primeira guia de Avaliação. Posteriormente, esses resultados servem para os demais sistemas, portanto, as demais guias de avaliação devem repetir o "resultado" indicado em relação ao Resultado da Contribuição com uma nota na Justificativa de que a avaliação é organizacional e refere-se à guia Avaliação - Sistema 1.

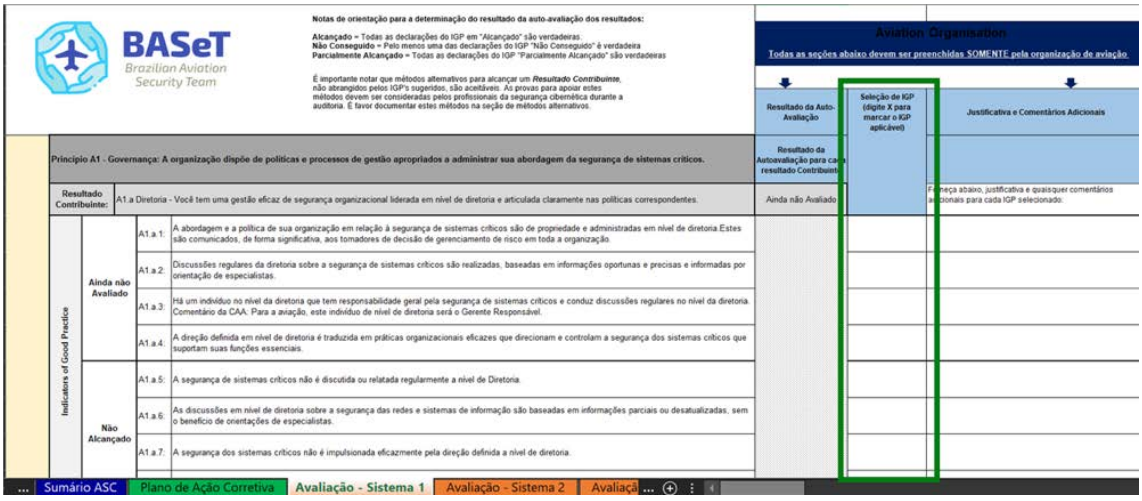
NOTA:

Quando se constata que vários sistemas críticos atendem aos mesmos Resultados Contribuintes e IGPs é aconselhável que eles estejam agrupados dentro da ASC, em consonância com o Manual de definição de escopo de sistemas críticos, para evitar duplicação da avaliação.

4.1. INDICADORES DE BOAS PRÁTICAS (IGP)

As organizações de aviação são obrigadas a usar os IGPs para avaliar suas funções essenciais e sistemas críticos contra cada Resultado Contribuinte.

Para indicar onde os IGPs estão sendo cumpridos, a organização de aviação deve marcar o IGP apropriado com um X:

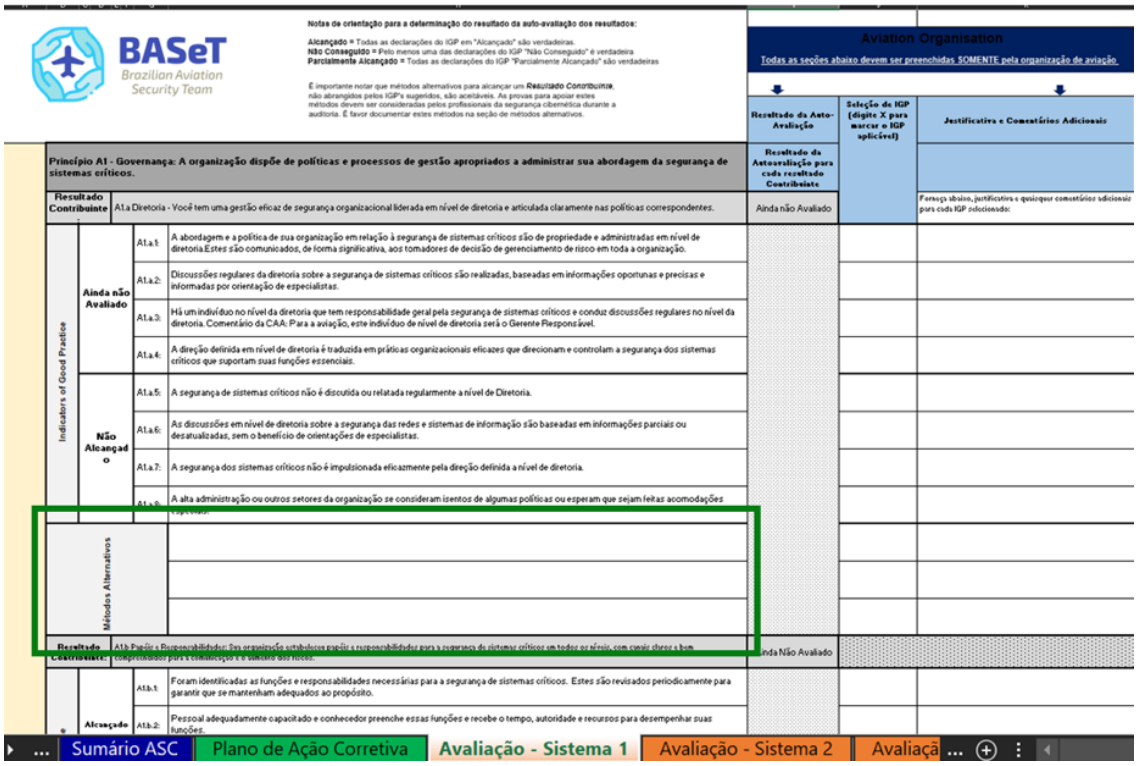


NOTA:

Em alguns casos, o Princípio é o Resultado Contribuinte. Isso acontece quando um Princípio possui apenas um Resultado Contribuinte. Nesses casos, a organização deve se referir ao Princípio associado.

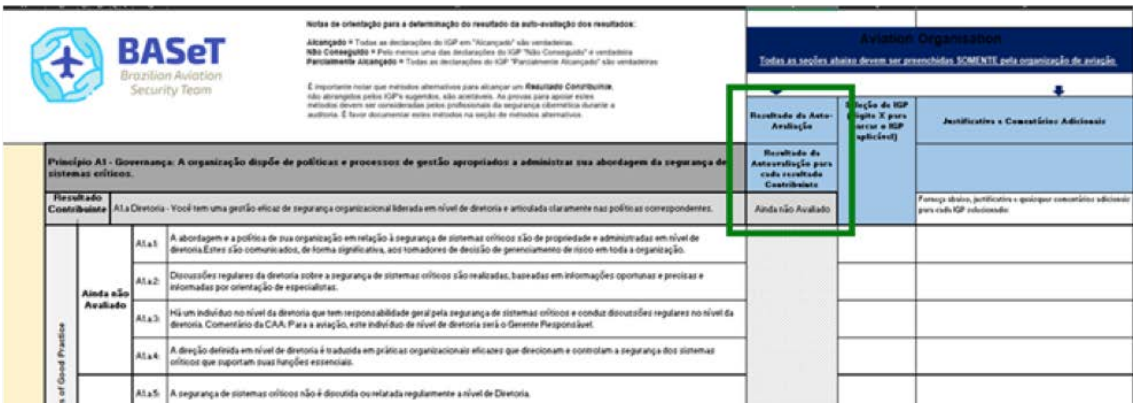
4.2. MÉTODOS ALTERNATIVOS

Entende-se que métodos alternativos (ou seja, boas práticas e controles adicionais), que não são cobertos pelos IGP's, mas ainda atendem ao Resultado Contribuinte podem estar sendo utilizados. Assim, estes devem ser detalhados nos campos "Métodos Alternativos".



4.3. RESULTADOS DE AUTOAVALIAÇÃO

Uma vez selecionados IGPs em relação a cada Resultado Contribuinte, a organização de aviação deve selecionar uma "Avaliação" no menu suspenso (*dropdown*).



A seleção de um status de avaliação deve ser feita de acordo com o seguinte critério:

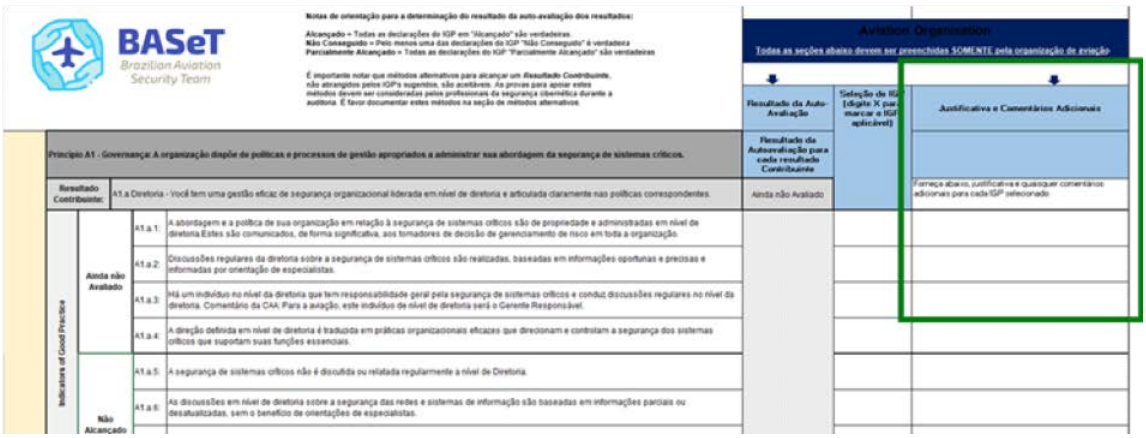
'Não Alcançado'	Deve ser selecionado **mesmo que apenas uma** declaração de IGP nesta coluna seja assinalada.
'Parcialmente alcançado'	**Só** pode ser selecionado se **todas** as declarações de IGPs nesta coluna forem assinaladas e se **nenhuma** declaração 'Não Alcançada' for apontada.
'Alcançado'	**Só** pode ser selecionado se **todas** as declarações de IGP nesta coluna forem assinaladas e se **nenhuma** declaração 'Não Alcançada' for assinalada.

Em determinadas circunstâncias, a seguinte opção pode ser escolhida no lugar das acima:

- 'Não relevante' (a justificativa **deve** ser fornecida onde esta for selecionada).

4.4. JUSTIFICATIVA DA ORGANIZAÇÃO DA AVIAÇÃO E COMENTÁRIOS ADICIONAIS

Após a seleção de IGPs e/ou Métodos Alternativos apropriados e o status de Avaliação, a organização de aviação deve usar a caixa de texto de preenchimento livre 'Justificativa e Comentários Adicionais' para fornecer fortes evidências narrativas para os selecionados do IGP.



5. PLANO DE AÇÃO CORRETIVA

A guia 'Plano de Ação Corretiva' permite que uma organização de aviação atribua planos de remediação às lacunas identificadas. Uma organização de aviação pode começar a desenvolver o Plano de Ação Corretiva e reunir informações enquanto realiza a autoavaliação inicial do CAF para a Aviação.

As organizações de aviação devem preencher a **coluna E** da guia 'Plano de Ação Corretiva' com a atribuição do perfil fornecido pela autoridade da aviação civil no Passo 1 do CAP 1753.

BASeT
Brazilian Aviation Security Team

PLANO DE AÇÃO CORRETIVA

Objetivos, Princípios e Contribuintes				Perfil (inserir perfil atribuído)	
Objetivo A: Gestão de Risco de Segurança	Princípio A1 - Governança	A1.a	Board de Diretores		Aind
		A1.b	Papéis e Responsabilidades		Aind
		A1.c	Decisor		Aind
	Princípio A2 - Gestão de Risco	A2.a	Processo de Gestão de Risco		Aind
		A2.b	Garantia		Aind
	Princípio A3 - Gestão de Ativos	A3.a	Gestão de Ativos		Aind
	Princípio A4 - Cadeia de Suprimentos	A4.a	Cadeia de Suprimentos		Aind
	Princípio B1 - Políticas e processos de proteção de serviços	B1.a	Desenvolvimento de Política e Processo		Aind
		B1.b	Implementação de Política e Processo		Aind
	Princípio B2 - Controle de Identificação e Acesso (CIA)	B2.a	Verificação de identidade, autenticação e autorização		Aind
		B2.b	Gestão de dispositivos		Aind
		B2.c	Gestão de Usuários Privilegiados		Aind

As organizações de aviação também devem detalhar da Coluna AE à AJ na guia 'Plano de Ação Corretiva' para cada Princípio e Resultado Contribuinte associado:

- Indicadores de Boas Práticas sendo abordados;
- Resumo de avaliação de risco do risco inerente e risco atual - incluindo detalhes das mitigações existentes;
- Nome do documento de evidência anexada de ações planejadas (por exemplo, orçamento e propriedade) ações (por exemplo, nome do documento do plano de projeto ou planos de remediação/mitigação de risco);
- Resumo de avaliação de risco da implementação do pós-plano de risco residual;
- Data de início (do trabalho de remediação/mitigação planejado); e
- Data estimada de conclusão (de trabalho de remediação/mitigação).

Informação de Ações Corretivas					
IBPs sendo tratados	**Resumo do risco inerente e do risco atual** (favor incluir detalhes das atenuações existentes)	**Nome do documento anexo com provas das ações planejadas** (deve incluir recursos, orçamento e propriedade)	**Resumo do risco residual** (pós implementação do plano)	**Data de início** (das ações planejadas)	**Data estimada de conclusão**

5.1. AVALIAÇÃO DE RISCO CIBERNÉTICO

As organizações de aviação devem seguir uma metodologia eficaz de avaliação de riscos cibernéticos ao realizar a correta análise para a conclusão de seu Plano de Ação Corretiva.

- Risco inerente é o nível de risco calculado por uma organização de aviação sem quaisquer atenuações no lugar.
- O risco atual é o nível de risco atual calculado por uma organização de aviação com mitigações em vigor (ou seja, as mitigações atuais em vigor no momento da conclusão da ASC).
- O risco residual é o nível estimado de risco de uma organização de aviação uma vez que as ações corretivas detalhadas no plano de ação corretiva foram implementadas.

Existem muitas metodologias a escolher para realizar uma avaliação de risco cibernético. As organizações de aviação são responsáveis pela seleção de uma metodologia adequada de avaliação de acordo com sua realidade. Recomenda-se que as seguintes áreas sejam consideradas na realização de avaliações de risco cibernético.

- Ameaças
- Vulnerabilidades
- Impacto (por exemplo, potenciais impactos na segurança)
- Probabilidade
- Mitigações e controles existentes

ANEXO A – REFERÊNCIAS INFORMATIVAS E EXEMPLO DE EVIDÊNCIAS

São fornecidas abaixo referências informativas e exemplos de evidências, os quais não são exaustivos, onde se acredita que boas práticas ou evidências alternativas que atendam a um Resultado Contribuinte, devam ser detalhadas na ASC no campo de "Métodos Alternativos".

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Gerenciamento de risco de segurança	**A1 Governança:** A organização tem políticas e processos de gestão adequados, em vigor, para governar sua abordagem para a segurança de sistemas críticos.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP 800-53 NIST SP 800-82 EUROCAE ED-204	- Detalhes das funções, responsabilidades, competências dos funcionários e autorizações de segurança apropriadas - Funções atribuídas a gerente geral e a gerente responsável por segurança cibernética - Estrutura de governança - Documentos da política de segurança cibernética - Abordagem de gerenciamento de riscos - Decisão de gerenciamento de risco documentada - Evidências de reuniões do conselho (por exemplo, agendas, atas)
	A2 Gestão de Risco: A organização toma as medidas apropriadas para identificar, avaliar e compreender os riscos de segurança para os sistemas críticos que suportam a operação das funções essenciais. Isso inclui uma abordagem organizacional geral para o gerenciamento de riscos.	ISO/IEC 27005:2018 ISO/IEC 27001:2017 ISO/IEC 3100:2018 ISA/IEC 62443 1-1 ISA/IEC 62443 2-1 NIST SP 800-30 NIST SP 800-37 NIST SP 800-39 NIST SP 800-82 EUROCAE ED202A, ED203A, ED204 & ED205 CyBOK Gerenciamento de Riscos & Área de Conhecimento de Governança	- Uso de métodos ou *frameworks* estabelecidos (por exemplo, ISO2700-X) Abordagem de gerenciamento de risco - Registros de revisão de avaliação de risco realizados de acordo com a governança de riscos - Uso de informações de ameaças e vulnerabilidades atuais no processo de avaliação de riscos - Registros de risco atual com ações associadas e plano de gerenciamento de melhoria (incluindo a propriedade do risco) - Evidências de atividade de garantia adequada

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Gerenciamento de risco de segurança	**A3 Gestão de Ativo:** Tudo o que é necessário para fornecer, manter ou suportar sistemas críticos está determinado e compreendido. Isto inclui dados, pessoas e sistemas, bem como qualquer infraestrutura de apoio (como energia ou refrigeração).	ISO/IEC 55001:2019 ISO/IEC27002: 2013 ISA 62443-1-1 NIST SP 800-82 NIST SP 800-53	- Política de gestão de ativos - Registro de ativos e verificação de amostra de ativos críticos através do ciclo de vida. Incluir ativos de TI e OT quando aplicável - Diagramas de arquitetura de rede de alto nível - Planos e roteiros para hardware e software, incluindo abordagem para *patches* e datas de fim de suporte
	A4 Cadeia de suprimentos: A organização entende e gerencia riscos de segurança para os sistemas críticos que suportam o funcionamento de funções essenciais que surgem como um resultado de dependências de fornecedores externos. Isto inclui garantir que as medidas apropriadas sejam empregadas onde os serviços de terceiros são utilizados.	ISO/IEC 27002:2013 ISO/IEC 27036-2 ISO/IEC 27036-3 ISA/IEC 62443-2-1 NIST SP 800-53 NIST SP 800-37 EUROCAE ED201	- Lista de fornecedores críticos mantidos incluindo seus contatos e responsabilidades de segurança cibernética - Detalhes dos requisitos de segurança cibernética impostos aos fornecedores - Visão geral dos acordos contratuais em vigor - Relatórios de avaliação completa e garantia de fornecedores
Protegendo contra ataques cibernéticos	**B1 Processos e políticas da função de proteção:** A organização define, implementa, comunica e impõe as políticas e processos apropriados que direcionam sua abordagem global para garantir sistemas e dados críticos que suportam a operação das funções essenciais.	ISO/IEC 27001:2017 ISO/IEC 27002:2013 ISO/IEC 22301:2019 ISA/IEC 62443-1-1 NIST SP 800-53 NIST SP 800-82	- Políticas, procedimentos e instruções de trabalho publicadas e controladas etc. - Procedimentos de RH que permitem a permissão adequada da segurança dos funcionários relevantes - Registros de configuração (por exemplo, para *firewalls*, etc.) - Registro de Gestão de mudanças - Política de Gestão de mudança - Registros de teste de validação - Relatórios de auditoria, relatórios de revisão e gerenciamento de ações resultantes

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Protegendo contra ataques cibernéticos	**B2 Identidade e controle de acesso:** A organização entende, documenta e gerencia o acesso a sistemas críticos que suportam o funcionamento de funções essenciais. Os usuários (ou funções automatizadas) que podem acessar dados críticos ou sistemas críticos são devidamente verificados, autenticados e autorizados.	ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP 800-53 NIST SP 800-82 EUROCAE ED204 Base de Conhecimento de Responsabilidades, Autenticação, Autorização da CyBOK	- Abordagem de autenticação e autorização adequada definida dentro de políticas de controle de acesso (incluindo para acesso físico, remoto e privilegiado) - Registros de usuários/ativos/contas autorizados atuais e o nível de acesso/privilégio atribuído a cada um (observando os requisitos de segurança de dados e gerenciamento de dispositivos) - Registros de revisões de direitos de acesso - Processos de admissão, movimentação e demissão de empregados documentados destacando controles de acesso baseados em funções
	B3 Segurança de dados: Os dados armazenados ou transmitidos eletronicamente estão protegidos de ações como acesso, modificação ou exclusão não autorizados que podem causar um impacto adverso em sistemas críticos. Essa proteção se estende aos meios pelos quais usuários autorizados, dispositivos e sistemas acessam dados críticos necessários para o funcionamento de sistemas críticos. Ele também cobre informações que ajudariam um invasor, como detalhes de design de sistemas críticos.	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP 800-53 NIST SP 800-82 EUROCAE ED204 & ED205	- Procedimentos relevantes para identificação e registro de dados e ativos sensíveis contendo esses dados e como estes são protegidos, incluindo o gerenciamento de dispositivos móveis, minimização de dados e limpeza remota - Detalhes sobre método de criptografia, incluindo algoritmos usados e gerenciamento de chaves - Registros de dados, serviços e conexões essenciais identificados e como estes são protegidos quando necessário, e avaliações de risco que suportam o nível de proteção aplicado - Declarações de impacto documentadas para perda ou alteração de dados que são regularmente revisadas, contendo planos de contingência quando necessário - Políticas de gerenciamento de informações documentadas detalhando retenção e exclusão

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Protegendo contra ataques cibernéticos	**B4 Segurança do sistema:** Sistemas críticos e tecnologia críticas para o funcionamento de funções essenciais estão protegidos contra ataques cibernéticos. Uma compreensão organizacional do risco para o sistema crítico informa o uso de medidas de segurança de proteção robustas e confiáveis para limitar efetivamente as oportunidades para os invasores comprometerem redes e sistemas.	ISO/IEC 27002:2013 ISA/IEC 62443-1-1 ISA/IEC 62443-2-1 ISA/IEC 62443-3-3 NIST SP 800-53 NIST SP 800-82 EUROCAE ED202A, ED203A, ED204 & ED205	- Política que estabelece requisitos de projeto para arquitetura, segregação e acesso a redes - Projetos de rede suportam monitoramento e recuperação de segurança eficazes - Procedimentos / instruções / modelos de vulnerabilidade / varredura e mitigação de ameaças visando reduzir a vulnerabilidade de ativos tais como aplicações, sistemas, infraestrutura, *firmware* etc (*hardening*) - Procedimentos de gerenciamento de *patches* e configuração de ativos Evidências da existência de uma lista (*whitelisting*) de softwares e componentes de softwares que tem o uso autorizado na organização e identificação de *malware*
	B5 Redes e sistemas resilientes: A organização constrói resiliência contra ataques cibernéticos e falhas do sistema no projeto, implementação, operação e gestão de sistemas críticos	ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-1-1 NIST SP 800-53 NIST SP 800-82	- Registros de revisão de limitações, restrições e fraquezas com evidência de revisão periódica - Estratégia documentada de Continuidade de Negócios e Recuperação de Desastres com evidências de práticas/testes que foram realizadas - *Software/firmware*/aplicativos/ configurações bibliotecas e cofres
	B6 Conscientização e Treinamento da Equipe: Os funcionários têm conscientização, conhecimento e habilidade apropriada para realizar suas funções organizacionais efetivamente em relação à segurança dos sistemas críticos que apoiam a operação das funções essenciais.	NSCS - 10 Passos: Educação e Conscientização do Usuário ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISA/IEC 62443-2-1 NIST SP 800-53 NIST SP 800-82	- Definição de requisitos de competência para funções e responsabilidades definidas em relação aos serviços essenciais - Treinamento de conscientização e/ou programas de educação em segurança cibernética - Registros de gestão de competências - Mecanismos de emissão de relatórios de mecanismos de segurança cibernética

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Detectando eventos de segurança cibernética	**C1 Monitoramento de segurança:** A organização monitora o estado de segurança da rede e dos sistemas que apoiam a operação de sistemas críticos, a fim de detectar possíveis problemas de segurança e rastrear a eficácia contínua das medidas de segurança de proteção.	NCSC - Introdução ao registro para propostas de segurança NCSC - 10 Passos: Monitoramento CREST – Guia de Monitoramento de Segurança Cibernética ISO/IEC 27002:2019 ISO/IEC 27002:2013 ISO/IEC 27035:1-3 ISA/IEC 62443-2-1 NIST SP 800-53 NIST SP 800-82 NIST SP 800-94	- Procedimentos que estabelecem requisitos de monitoramento de segurança, incluindo, resolução de incidentes, requisitos de assinatura de *malware/IoC* e recursos em quantidade e qualidade adequadas (*resourcing*) - Registros de monitoramento periódico (por exemplo, de registros de segurança, registros de detecção de vírus, registros de detecção de intrusões etc.) - Análise e interpretação da inteligência de ameaças e registros periódicos de monitoramento e gestão de ações resultantes - A fidelidade dos dados registrados permite informar a função de proteção, e por si só que está adequadamente protegida contra alterações não autorizadas, está corretamente e seguramente correlacionada, e o acesso aos registros é atribuído a usuários únicos - Evidências de indicadores de ameaças *(threat intelligence feeds)* estarem disponíveis à organização e poderem ser compartilhados quando necessários
	C2 Detecção de eventos de segurança proativa: A organização detecta, dentro de sistemas críticos, atividades maliciosas que afetam ou com o potencial de afetar, o funcionamento de funções essenciais mesmo quando a atividade evita soluções padrão de prevenção/ detecção de segurança baseadas em assinatura (ou quando as soluções padrão não são implantáveis).	ISO/IEC 27001:2019 ISO/IEC 27002:2013 ISO/IEC 27035-3 ISA/IEC 62443-2-1 NIST SP 800-53	- Procedimentos que estabelecem requisitos de monitoramento de segurança, incluindo métricas de desempenho (*beselining*) de rede e detecção de código malicioso - Registros de monitoramento periódico alimentando processos de inteligência e monitoramento de ameaças (por exemplo, de registros de segurança, registros de detecção de vírus, registros de detecção de intrusões etc.) - Análise e interpretação de eventos de inteligência de ameaças e monitoramento de rede, registros periódicos de monitoramento e gerenciamento de ações resultantes - Detalhamento de processos em busca de ameaças ou anormalidades dentro de sistemas críticos e suas documentações, incluindo avaliações de riscos relevantes

Objetivo	Princípio	Referências Informativas	- Exemplo de Evidência
Minimizando o impacto dos incidentes de segurança cibernética	**D1 Plano de resposta e recuperação:** Existem processos de gerenciamento de incidentes bem definidos e testados, em vigor, que visam garantir a continuidade das funções essenciais nos sistemas de eventos ou em caso de falha de serviço. Atividades de mitigação destinadas a conter ou limitar o impacto do compromisso também estão em vigor.	NCSC -10 Passos: Gerenciamento de Incidentes ISO/IEC 27035 (todos) ISO/IEC 22301:2019 ISO/IEC 27002:2013 NIST SP 800-61 NIST SP 800-53 NIST SP 800-82 EUROCAE ED204	- Plano de resposta a incidentes atualizados, aprovado e compreensivo detalhando ataques, papéis e responsabilidades conhecidos e possíveis que abranjam o ciclo de vida de um incidente - Planos de exercício de resposta a incidentes baseados em inteligência e eventos de ameaças relevantes, que são regularmente revisados e validados
	D2 Lições aprendidas: Quando um incidente ocorre, são tomadas medidas para entender suas causas básicas e garantir que ações adequadas de correção sejam tomadas para proteger contra incidentes futuros.	NCSC - 10 Passos: Gerenciamento de Incidentes ENISA - Boas Práticas para Orientação de Gerenciamento de Incidentes ISO/IEC 27035:2-3 ISO/IEC 22301:2019 ISO/IEC 27001:2019 ISO/IEC 27002:2013 NIST SP 800-61 NIST SP 800-53	- Evidências de análise de causas básicas pós-incidente compreensiva que é conduzida rotineiramente, que abrange a política organizacional, bem como problemas/vulnerabilidades de hardware/software - Política de revisão de incidentes documentada detalhando os requisitos das lições aprendidas - Evidências que mostram as lições aprendidas alimentando a melhoria contínua

ANAC AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL

BASeT
Brazilian Aviation Security Team