MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

GOVERNANÇA

PCA 16-14

PLANO DE ADEQUAÇÃO DO COMANDO DA AERONÁUTICA À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

2021

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

GOVERNANÇA

PCA 16-14

PLANO DE ADEQUAÇÃO DO COMANDO DA AERONÁUTICA À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

2021

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

PORTARIA EMAER Nº 93/CEMAER, DE 21 DE DEZEMBRO DE 2021.

Aprova o Plano que dispõe sobre a adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados Pessoais.

O CHEFE DO ESTADO-MAIOR DA AERONÁUTICA, no uso das atribuições que lhe confere o inciso II do Art. 20 do ROCA 20-5 "Regulamento do Estado-Maior da Aeronáutica", aprovado pela Portaria GABAER nº 38/GC3, de 5 de fevereiro de 2021, resolve:

Art. 1º Aprovar o PCA 16-14 "Plano de adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados Pessoais", que com esta baixa.

Art. 2º Esta Portaria entra em vigor no dia 03 de janeiro de 2022.

Ten Brig Ar MARCELO KANITZ DAMASCENO
Chefe do Estado-Maior da Aeronáutica

(Publicada no BCA nº 237, de 28 de dezembro de 2021.)

SUMÁRIO

PREFÁCIO

Inspirada no modelo europeu, o *General Data Protection Regulation* (GDPR), a Lei Geral de Proteção de Dados Pessoais (LGPD) foi constituída a fim de garantir maior segurança jurídica à privacidade e ao uso de dados pessoais no território brasileiro, de modo que é basilar para que se modifiquem paradigmas em relação à coleta e ao tratamento dos dados pessoais. Além disso, a LGPD assegura uma série de direitos aos titulares dos dados pessoais, sendo aplicada a todas as organizações, independentemente do porte, regime jurídico ou natureza dos dados pessoais manipulados. Logo, todos devem efetuar alterações em seus processos para que consigam se adequar à legislação brasileira de proteção de dados.

Dentre as inovações jurídicas, recaímos sobre a necessidade de implementar um Programa de Governança em Privacidade à luz da LGPD, vez que esta Lei está em vigor desde agosto de 2020. Para que o programa de governança em privacidade esteja adequado ao cenário atual de tratamento de dados é preciso considerar a proteção dos dados pessoais um ativo estratégico, pois auxiliará a organização não só no que tange às sanções administrativas previstas na Lei, mas também ao aumento do grau de confiabilidade da sociedade e dos próprios militares na maneira com que a Força Aérea Brasileira (FAB) trata seus dados pessoais.

Com a vigência da LGPD, as organizações perceberam a importância da criação de um programa de governança em privacidade, exemplificado pela Diretriz do Comando da Aeronáutica (DCA 16-6), entendendo de forma clara as etapas mínimas a serem executadas e a correta priorização das ações necessárias para a devida implementação do programa. Com isso, diante da realidade do Comando da Aeronáutica (COMAER), a execução deste plano de ação será determinante para que sejam definidas as atividades necessárias e para que os processos de negócio estejam em conformidade com a LGPD.

Deste modo, o Estado-Maior da Aeronáutica (EMAER) e a Diretoria de Tecnologia da Informação da Aeronáutica (DTI), com o suporte da consultoria prestada pela empresa *EVERY CYBERSECURITY AND GRC (Governance, Risk Management, and Compliance)*, realizaram o inventário dos principais macroprocessos da FAB que tratam de dados pessoais.

Esse inventário evoluiu para um diagnóstico que resultou nas ações corretivas sugeridas ao longo deste Plano. Tudo sustentado com uma metodologia consonante com as melhores práticas recomendadas e vigentes, até que o primeiro ciclo do programa de adequação, que ora se inicia, seja completado.

Este plano também representa a materialização da Governança, pois foi possível avaliar o nível de maturidade do COMAER no tratamento de dados pessoais, direcionar a um aprimoramento daquelas ações que necessitam de adequação e, com a publicação deste normativo, será feito o monitoramento, em caráter preventivo, na direção da conformidade.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

A finalidade precípua da presente publicação de adequação do Comando da Aeronáutica à Lei Geral de Proteção de Dados Pessoais é consolidar e detalhar as ações identificadas durante a realização da análise dos processos de negócio, estabelecendo um plano de ação para atendimento aos requisitos regulatórios da LGPD.

1.2 CONCEITUAÇÕES

Os termos e expressões empregados neste documento constam no Glossário da Aeronáutica (MCA 10-4), no Glossário das Forças Armadas (MD35-G-01) e no Artigo 5º da LGPD.

1.3 ÂMBITO

Este plano aplica-se a todas as Organizações do Comando da Aeronáutica.

2 METODOLOGIA APLICADA

A seguir será descrita a metodologia utilizada para entendimento e registro dos processos que tratam dados pessoais no COMAER.

2.1 IDENTIFICAÇÃO DAS LACUNAS

2.1.1 A metodologia aplicada foi o da análise das lacunas (do inglês *GAP ANALYSIS*) entre o estado atual do COMAER e o cenário que se pretende atingir quanto à conformidade com a Lei Geral de Proteção de Dados Pessoais.

2.1.2 Esse método fornece uma maneira de identificar estratégias, estruturas, capacidades, processos, práticas, tecnologias ou habilidades insuficientes ou ausentes, para então recomendar a execução de ações que ajudarão a organização a atingir suas metas.

2.1.3 Segundo o *Gartner*, empresa global de consultoria e pesquisa, em seu relatório *Beyond GDPR: 5 Best Practices for LGPD Compliance*, a realização de um *Gap Analysis* é uma das etapas fundamentais para a implementação bem-sucedida de um Programa de Governança em Privacidade em uma organização. Dessa forma, e com o objetivo de adequação das atividades e processos da FAB aos requisitos de tratamento de dados pessoais propostos pela LGPD, a realização do *Gap Analysis* se configurou como etapa essencial deste projeto.

2.2 IDENTIFICAÇÃO DO ESTADO ATUAL

2.2.1 Inicialmente, é necessário registrar o estágio atual do COMAER quanto à adequação à legislação de privacidade e proteção de dados pessoais. Indica-se, portanto, como as áreas têm incorporado o tema aos seus processos, após a realização de atividades que permitiram essa avaliação – análise de documentos e dados, estruturados ou não, processos internos, base de dados e sistemas que realizam tratamento de dados pessoais.

2.2.2 De maneira geral, verificou-se a necessidade de tratamento específico da temática de privacidade e proteção de dados pessoais no que se refere às obrigações e responsabilidades das partes, o que implica em constante dever de vigilância em relação às práticas adotadas para proteção dos dados pessoais compartilhados pela FAB.

2.2.3 Por sua vez, foram avaliados os dados pessoais que atualmente são tratados pelos diversos Órgãos de Direção Geral, Setorial e Assessoria Direta ao Comandante da Aeronáutica (ODGSA). Durante esta fase foram realizadas reuniões de levantamento das informações, inclusive com elos técnicos, nas quais foram coletadas informações acerca do ciclo de vida do tratamento desses dados pessoais.

2.2.4 No tocante à análise documental, foram avaliados documentos dos mais diversos tipos, relacionados a atividades executadas pelas áreas entrevistadas durante o levantamento de informações. A partir dessa avaliação, foram redigidas recomendações pertinentes para a adequação dos processos de negócio e tratamentos decorrentes da Lei 13.709/2018.

2.2.5 Também, para melhor compreensão do cenário atual do COMAER, foram realizadas avaliações de riscos nos principais sistemas da informação que realizam o tratamento de dados pessoais. Esta avaliação elencou os principais riscos à privacidade presentes nos sistemas avaliados.

2.2.6 Em linhas gerais, nos processos avaliados foram identificados que alguns pontos de atenção da LGPD já estavam contemplados, mas outros ainda precisam ser desenvolvidos ou melhorados, para que seja alcançada à conformidade com a Lei. Especialmente, mas não somente, em relação à temporalidade, destinação final e utilização de controles físicos ou lógicos, foi possível visualizar lacunas de adequação que precisarão ser corrigidas. Para auxiliar neste processo, serão apresentadas as ações recomendadas ao longo deste Plano.

2.3 IDENTIFICAÇÃO DO CENÁRIO PRETENDIDO

2.3.1 Verificado o estado atual, é importante identificar também o cenário que a organização pretende atingir após o empreendimento de esforços para eliminar as falhas e pontos de atenção apontados.

2.3.2 O cenário pretendido representa a condição ideal em que a organização deseja estar. Deste modo, o resultado almejado é a conformidade dos processos de negócio do COMAER aos requisitos e regramentos da Lei Geral de Proteção de Dados Pessoais, de maneira que as ações a serem implementadas terão como fundamento a própria Lei e os normativos internos, a fim de preparar a organização para sua aplicação e eventuais acionamentos da Autoridade Nacional de Proteção de Dados (ANPD).

2.3.3 Com esse objetivo estabelecido, por mais que possa parecer muito amplo, demanda que ações altamente específicas sejam implementadas no âmbito de cada um dos processos avaliados e, através do somatório alcançado com a implementação de todas as ações, permita à FAB alcançar o patamar pretendido ao final deste primeiro ciclo.

2.4 LACUNAS IDENTIFICADAS

2.4.1 Após identificar o estado atual e onde se deseja chegar, é possível conhecer os *Gaps* ou lacunas existentes nos processos avaliados, que podem ser compreendidos como a diferença entre os dois estágios.

2.4.2 Como a LGPD trata do tema proteção de dados pessoais e não havia, até então, uma lei ou normativo específico que tratasse sobre este assunto, muitos dos processos do COMAER aqui avaliados não possuem ainda controles implementados especificamente para a proteção de dados pessoais e privacidade.

2.4.3 A ausência de controles específicos voltados para o atendimento à LGPD e seus aspectos de privacidade mostram lacunas no modo em que a FAB tem tratado os dados pessoais.

2.4.4 Superadas essas lacunas, além da conformidade com a LGPD, será possível atingir um maior nível de segurança e de proteção, não somente com os dados pessoais em tratamento, mas também com diversos outros tipos de dados.

2.4.5 Com base no diagnóstico realizado, foram identificados dois tipos de *Gaps* na forma com que o COMAER realiza as operações de tratamento de dados pessoais em seus processos de negócio.

2.4.5.1 *Gaps* de Segurança

a) ausência de controles criptográficos;

b) ausência de controles de acesso lógico;

c) ausência de controles de segurança em redes, proteção física e do ambiente;

d) ausência de mecanismos de desenvolvimento seguro;

e) ausência de mecanismos para registro de eventos, rastreabilidade e salvaguarda de *logs*;

f) ausência de mecanismos para garantir a segurança *web*; e

g) ausência de procedimento de resposta a incidentes.

2.4.5.2 *Gaps* de Privacidade

a) ausência de mecanismos de conscientização sobre a importância da privacidade e segurança da informação;

b) ausência de mecanismos de consentimento e escolha;

c) ausência de mecanismos para garantir a precisão e a qualidade;

d) ausência de medidas de responsabilização;

e) ausência de medidas para assegurar a limitação da coleta;

f) ausência de medidas para assegurar o *compliance* com a privacidade;

g) ausência de medidas para garantir a abertura, transparência e notificação; e

h) ausência de tabela de temporalidade e destinação final definidas.

2.4.6 Cada um dos *Gaps* identificados pode estar associado a um ou mais controles que serão posteriormente propostos para a sua correção. O objetivo dessa análise é a apresentação das principais deficiências identificadas no tratamento de dados pessoais, bem como os insumos que possibilitem a seleção das lacunas de maior risco a serem corrigidas.

2.4.7 No Anexo B é possível observar os dados estatísticos do quantitativo das ações de conformidade distribuídas em função dos *Gaps*.

3 MAPA DE RISCO

O Mapa de Risco é uma representação que permite reconhecer, de maneira simples e objetiva, os riscos presentes em determinadas atividades, no tocante ao modo como os dados pessoais estão sendo tratados e se estão em concordância com a LGPD. Tudo por meio da identificação da probabilidade e do impacto da não conformidade no processo de adequação, realçada pelas considerações aos parâmetros da DCA 16-2, que trata da Gestão de Risco no COMAER, com algumas adaptações para esse processo específico.

3.1 PROBABILIDADE (P)

3.1.1 A avaliação de riscos fornece o entendimento apropriado de como estes processos poderiam afetar a adequação do COMAER à LGPD, bem como a eficácia dos controles propostos.

3.1.2 A probabilidade será aplicada sobre os processos levantados que representam o maior impacto na tarefa de adequação com a LGPD e serão divididas em três gradações:

a) **Alta** (3): devido à presença de diversos fatores de riscos, o que pode impactar na manutenção da privacidade dos dados pessoais por ela tratados;

b) **Moderada** (2): devido à presença de alguns fatores de riscos, o que ainda pode representar um impacto na manutenção da privacidade dos dados pessoais tratados pelo COMAER; e

c) **Baixa** (1): devido ao número baixo (ou ausência) dos fatores de risco aqui elencados que podem impactar a FAB na manutenção da privacidade dos dados pessoais tratados.

3.1.3 Para o enquadramento nas gradações destacadas no item anterior será necessária a realização de algumas perguntas, conforme considerações da tabela 1, que ajudarão a identificar a presença (ou não) destes fatores de riscos em cada processo.

Perguntas	Considerações
O processo trata dados pessoais sensíveis?	A LGPD garante que o tratamento de dados pessoais sensíveis se dará somente em determinadas hipóteses e de maneira que se adote medidas de segurança, técnicas e administrativas compatíveis com a devida proteção de tais informações. Não havendo a adoção de tais medidas ou, havendo, mas de maneira insuficiente para que se tenha proteção adequada dos dados pessoais sensíveis, há que se falar em risco. Neste sentido, percebe-se a importância da identificação de processos que tratem dados pessoais sensíveis e dos riscos a eles vinculados, uma vez que ao identificar tal lacuna, a FAB poderá atuar preventivamente e diminuir as possibilidades de vazamento ou tratamento indevido de referidas informações.
O processo possui temporalidade e destinação final definidas?	O artigo 15, inciso I, da LGPD afirma que o término do tratamento de dados pessoais ocorrerá quando se verificar o alcance da finalidade para o tratamento de tais informações. Isso significa que o COMAER deverá estar atento não só a este alcance, mas também à toda coleta de dados pessoais para tal finalidade, destinação final, possível esgotamento do prazo definido como temporalidade para utilização do dado e, inclusive, eventual alteração de finalidade. Por este motivo é de suma importância que sejam cumpridos os normativos e regulamentos dedicados aos prazos de guarda e destinação

	final para determinar os níveis de riscos aos quais os processos estão suscetíveis. Além disso, tal definição permite que a organização somente tenha sob sua posse os dados pessoais que realmente são necessários para a execução de suas atividades.
O processo coleta dados além dos mínimos necessários?	O dever de garantia do princípio da necessidade está previsto no artigo 6º, inciso III da LGPD, o qual é bem definido no Guia de Boas Práticas da LGPD como "o direito à limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento". Compreende-se que o simples fato de coletar dados além do estritamente necessário para realização e bom desenvolvimento de determinada atividade ou processo, pode oferecer risco desnecessário para a organização. Sendo assim, recomenda-se que o COMAER colete apenas os dados se justificarem como imprescindíveis para a realização de suas atividades, uma vez que a coleta excessiva lhe trará maior responsabilidade quanto ao devido tratamento dos dados pessoais, e consequentemente, maior risco à organização. Portanto, o risco pode ser facilmente mitigado com a coleta de informações estritamente necessárias para execução dos processos.
O processo possui algum tipo de tratamento realizado por terceiros/fontes externas?	A norma de proteção de dados pessoais brasileira traz em seus artigos as reponsabilidades e a possibilidade de eventual ressarcimento de danos por aqueles que realizarem o tratamento de dados pessoais de maneira indevida. Neste sentido, cabe igualmente aos operadores de dados pessoais a responsabilidade pelo tratamento de tais informações. Quando houver algum tipo de tratamento realizado por terceiros/fontes externas, a organização precisa verificar se os referidos operadores tratam tais informações de maneira correta. Dessa forma, o COMAER deverá agir de forma proativa, preventiva e responsável sobre tais informações, para que em caso de vazamento ou tratamento de maneira inadequada, ela possa se resguardar e proteger os dados pessoais que estão sob sua responsabilidade. O simples fato de um terceiro realizar tratamento de dados pessoais que estejam sob a responsabilidade da FAB, por si só já é um ponto de atenção que a organização precisa estar atenta para que não gerem riscos desnecessários.
O processo tem mecanismos de rastreabilidade de seus dados?	Em caso de tratamento incorreto ou violação de dados pessoais, há que se buscar não só o responsável pelo incidente, mas também o caminho que se deu até que essa violação ocorresse. Ao possuir mecanismos de rastreabilidade, a mitigação de riscos torna-se mais eficiente e efetiva, uma vez que o rastreamento facilita a identificação e análise do erro cometido. A identificação do agente causador do erro, data e horário da violação, por exemplo, permitem que o evento causador da violação seja rastreado e haja a identificação do momento exato que houve a violação de privacidade, podendo ser tratada em tempo hábil para que não ocorra reincidências e maiores prejuízos aos titulares daquelas informações.

Tabela 1 – Perguntas para avaliação da probabilidade de Risco.

3.1.4 Uma vez apresentados os fatores de riscos a serem avaliados quanto a probabilidade, compreende-se, portanto, a necessidade de se respondê-las de maneira correta e com precisão para que os riscos de não adequação e conformidade com a LGPD sejam mitigados.

3.1.5 Cada um dos critérios, ou fatores de riscos aqui apresentados, podem possuir, ou não, pesos semelhantes devido à importância estabelecida à tal fator para a manutenção da privacidade. Por exemplo, o fato de um processo ter o tratamento de seus dados realizado por outras empresas representa um risco à manutenção da privacidade, porém se esta empresa também cuida dos aspectos relacionados à proteção dos dados, certamente este fator não terá um impacto tão grande para a FAB. Por outro lado, um processo cujo tratamento dos dados pessoais não possui minimamente os quesitos de rastreabilidade, representará certamente um grande risco de violação a estes dados.

3.1.6 Diante do exposto e com base em todo o mapeamento realizado durante a etapa de diagnóstico e análise de inventário de dados pessoais, foi realizado uma avaliação da probabilidade dos fatores de riscos presentes em cada um dos processos identificados, por meio do Registro das Operações de Tratamento de Dados (RTD). Este resultado é expresso através da tabela a seguir.

Nº RTD	Processo	Responsável	São tratados dados pessoais sensíveis?	Há temporalidade e destinação final definidas?	São coletados dados além dos mínimos necessários?	Há algum tipo de tratamento realizado por terceiros/fontes externas?	Há mecanismos de rastreabilidade de seus dados?	Probabilidade
1	Desenvolvimento e manutenção de sistemas	CCA-RJ	Sim	Não se aplica	Não	Sim	Não	Moderada
2	Concessão de VPN	CCA-RJ	Não	Não	Não	Não	Não	Moderada
3	Registro e tratamento de incidentes de rede	CCA-BR	Não	Não	Não	Não	Não	Moderada
4	Gestão do sistema de informação gerencial de apoio à decisão da Aeronáutica	CCA-BR	Sim	Não	Não	Não	Não	Alta
5	Análise de mérito	SECPROM	Não	Não se aplica	Não	Não	Não	Baixa
6	Avaliação de desempenho de oficiais e graduados	SECPROM	Sim	Não	Não	Não	Não	Alta
7	Consultoria e assessoramento jurídico	COJAER	Sim	Não	Não	Sim	Sim	Moderada
8	Gerir processos judiciais de interesse do COMAER	COJAER	Sim	Não	Não	Sim	Não	Alta
9	Aplicação do teste de avaliação do condicionamento físico para exames de admissão e de seleção	CDA	Sim	Não	Não	Não	Não	Alta

10	Teste de avaliação do condicionamento físico	CDA	Sim	Não se aplica	Não	Não	Não	Moderada
11	Credenciamento de segurança para utilização da rede mercúrio	CIAER	Sim	Não	Não	Não	Sim	Moderada
12	Realizar investigação de ocorrências aeronáuticas	CENIPA	Sim	Parcial	Não	Sim	Não	Alta
13	Realizar ações de prevenção de ocorrências aeronáuticas	CENIPA	Não	Parcial	Não	Sim	Não	Moderada
14	Pós formação de graduados e oficiais de carreira	DIRENS	Não	Não	Não	Não	Não	Moderada
15	Processo seletivo	DIRENS	Sim	Parcial	Não	Não	Não	Moderada
16	Promover informações aos cidadãos	CECOMSAER	Não	Não	Não	Sim	Sim	Moderada
17	Relacionamento com a imprensa	CECOMSAER	Não	Não	Não	Não	Não	Moderada
18	Gerenciamento da saúde complementar	DIRSA	Sim	Não	Não	Sim	Não	Alta
19	Análise de procedimentos de alto custo e ressarcimento de despesas no exterior	DIRSA	Sim	Não	Não	Sim	Não	Alta
20	Julgamento de recursos da junta superior de saúde	DIRSA	Sim	Parcial	Não	Não	Não	Moderada
21	Cadastro de beneficiários do sistema de saúde da aeronáutica	DIRSA	Sim	Parcial	Não	Não	Não	Moderada
22	Obter serviços de tráfego aéreo (ATS)	DECEA	Não	Não	Não	Não	Não	Moderada
23	Solicitar autorização para voo de aeronaves remotamente pilotadas	DECEA	Não	Não	Não	Não	Não	Moderada
24	Formação e capacitação dos recursos humanos do Sistema de Controle do Espaço Aéreo Brasileiro	ICEA	Não	Não	Não	Não	Não	Moderada
25	Planejar e executar auditorias e fiscalizações	CENCIAR	Sim	Não	Não	Sim	Não	Alta
26	Tomada de contas especial (TCE)	CENCIAR	Não	Não	Não	Sim	Não	Alta
27	Realização de Exames de Aptidão Psicológica	IPA	Sim	Parcial	Não	Não	Não	Moderada
28	Indicações para missões internacionais	COMAE	Não	Sim	Não	Não	Não	Baixa
29	Emissão do Boletim do Comando da Aeronáutica (BCA)	CENDOC	Não	Sim	Não	Não	Não	Baixa

30	Gestão do arquivo intermediário	CENDOC	Sim	Sim	Não	Não	Não	Moderada
31	Gestão do arquivo permanente	CENDOC	Sim	Sim	Não	Não	Não	Moderada
32	Gerenciar a segurança e defesa das instalações da Aeronáutica	COMPREP	Não	Não	Não	Não	Não	Moderada
33	Prospectar oportunidades	DCTA	Não	Não	Não	Não	Não	Moderada
34	Gerir parcerias	DCTA	Não	Não	Não	Sim	Não	Alta
35	Gerir pagamento de pessoal	DIRAD	Não	Não	Não	Sim	Não	Alta
36	Administração de próprios nacionais residenciais	DIRAD	Sim	Não	Não	Não	Não	Alta
37	Gestão de hotelaria	DIRAD	Não	Não	Não	Não	Não	Moderada
38	Gestão de instrumentos de parceria	DIREF	Não	Sim	Não	Não	Não	Baixa
39	Outorga de procuração para representação financeira	DIREF	Não	Sim	Não	Sim	Não	Moderada
40	Demissão ou transferência para a reserva remunerada de oficial/graduado	DIREF	Não	Não	Não	Não	Não	Moderada
41	Atualização de registro de danos ao erário	DIREF	Não	Não	Não	Sim	Não	Alta
42	Cadastro de usuários em sistemas corporativos do Poder Executivo Federal	DIREF	Não	Não	Não	Sim	Não	Alta
43	Suportar a estrutura administrativa do Comandante	GABAER	Não	Não	Não	Não	Não	Moderada
44	Gerenciar medalhas e condecorações	GABAER	Sim	Não	Não	Não	Não	Alta
45	Relacionar-se com os poderes Executivo, Legislativo e Judiciário	ASPAER	Não	Não	Não	Não	Não	Moderada
46	Gerir compras	CAE	Não	Não	Não	Sim	Não	Alta
47	Gestão de inativos e pensionistas	BREVET	Sim	Não	Não	Não	Não	Alta
48	Inspeções de segurança nos provedores de serviços de navegação aérea	ASOCEA	Não	Não	Não	Não	Não	Moderada
49	Indicação de militares para missões de paz	EMAER	Sim	Não	Não	Sim	Não	Alta
50	Gestão de dados dos auxiliares locais nas adidâncias	EMAER	Não	Não	Não	Não	Não	Moderada
51	Autorização de voo no espaço aéreo brasileiro	EMAER	Não	Não	Não	Não	Não	Moderada

52	Gestão do programa forças no esporte	EMAER	Não	Não	Não	Sim	Não	Alta
53	Declaração de bens e valores	SEFA	Não	Não	Não	Não	Não	Moderada
54	Prestação de tarefa por tempo certo	COMGEP	Sim	Não	Não	Não	Não	Alta
55	Desenvolvimento e manutenção de sistemas	CCA-BR	Sim	Não se aplica	Não	Não	Não	Moderada
56	Desenvolvimento e manutenção de sistemas	CCA-SJ	Sim	Não se aplica	Não	Não	Não	Moderada

Tabela 2 – Relação dos processos (Registro das Operações de Tratamento de Dados - RTD) e respectiva avaliação da probabilidade de risco.

3.2 IMPACTO (I)

3.2.1 Após a análise da Probabilidade, o outro fator importante na análise geral do risco é a observação do "impacto" representado pela severidade da ação analisada, caso o processo de adequação não seja executado.

3.2.2 Esse critério é baseado nos requisitos apresentados pela LGPD e são divididos conforme a seguir:

a) **Impacto Alto** (3): trata-se de um item **obrigatório** apresentado na lei e que é fundamental estar implementado para que seja possível considerar o COMAER em conformidade com a LGPD;

b) **Impacto Moderado** (2): trata-se de um item apresentado na lei, porém sua implementação é **sugerida** para a conformidade com a LGPD; e

c) **Impacto Baixo** (1): trata-se de item que não é referenciado diretamente na lei, porém, sua implementação representa a aplicação das **melhores práticas** que trará um maior nível de proteção aos dados pessoais.

3.3 RISCO (R)

3.3.1 Ao final da atribuição de notas para esses indicadores, faz-se necessário produzir um índice que definirá qual o grau de prioridade de cada ação para o processo de adequação destes processos à LGPD.

3.3.2 O cálculo do índice de Risco, também nomeado como índice de Gravidade ou de Criticidade, é realizado através da multiplicação dos dois indicadores previamente pontuados, ou seja, *Risco (R)= Probabilidade (P)* X *Impacto (I).*

3.3.3 Este indicador pode variar entre 1 (1 x 1) e 9 (3 x 3) o que facilita a ordenação dos controles. Caso existam controles com o mesmo valor, e ainda assim, for necessário algum tipo de priorização entre eles, é recomendável que seja priorizado aquele que possuir o maior grau de severidade ou impacto.

3.3.4 Uma forma de se apresentar estes controles é através de um mapa de calor, o que auxilia na visualização do que realmente é prioritário e dá uma visão geral de quão crítica é a atual situação dos processos em relação à proteção dos dados pessoais.

3.3.5 O mapa de calor apresentado a seguir (Figura 1) contém o quantitativo distribuído por criticidade identificada nas ações e nos controles diagnosticados, bem como sugeridos neste Plano de Ação.

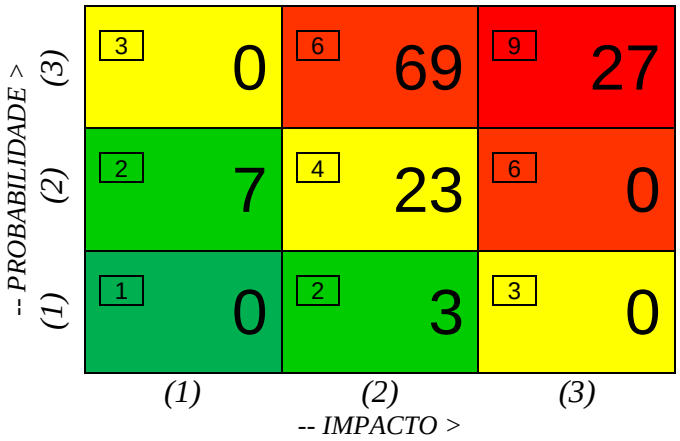

Figura 1 – Mapa de calor contendo a distribuição das ações diagnosticadas em função do Risco.

3.3.6 No Anexo B também é possível observar os dados estatísticos do quantitativo das ações de conformidade distribuídas em função do Risco.

3.3.7 Ao avaliar as ações no mapa de calor, percebe-se que o número de ações críticas (níveis de criticidade 6 e 9) representam um quantitativo significante para os processos analisados. Isto ocorre devido à relevância das informações tratadas nestes processos, bem como pelo curto prazo que as áreas responsáveis pelos processos possuem para implementá-las.

3.3.8 Uma vez que estes controles estão priorizados, é necessário que sejam distribuídos para que cada equipe tenha o correto entendimento do esforço que será necessário na sua execução e, assim, definirem uma estratégia de implementação.

4 PLANEJAMENTO DAS AÇÕES DE ADEQUAÇÃO

4.1 CONTROLES

4.1.1 Após identificar os *Gaps* existentes nos processos e realizar a avaliação do risco inerente, o próximo passo será a divisão dos processos de acordo com o conjunto de controles a serem estabelecidos, a partir dos resultados obtidos com o diagnóstico necessário para a melhoria dos processos.

4.1.2 Os controles adotados para o planejamento das ações de adequação no COMAER serão os seguintes:

a) **Controles Legais e Normativos**: controles relacionados a alterações de normativas internas e contratos que dão suporte às atividades do ciclo de vida dos dados pessoais;

b) **Controles Processuais**: controles relacionados a criações ou alterações de processos, políticas e definições de regras de negócios que afetem as atividades do ciclo de vida dos dados pessoais; e

c) **Controles Tecnológicos**: controles relacionados a criações ou adequações dos sistemas e ou portais do COMAER.

4.1.3 No Anexo B é possível observar os dados estatísticos do quantitativo das ações de conformidade distribuídas em função dos Controles.

4.2 PLANO DE AÇÃO PARA A CONFORMIDADE

4.2.1 A Resolução do Conselho Diretor da Autoridade Nacional de Proteção de Dados (CD/ANPD nº1, de 28 de outubro de 2021) aprovou no Art. 36 os itens mínimos que devem conter em um plano de conformidade, ao colocarem em prática seu processo de fiscalização.

4.2.2 Neste sentido, o COMAER fará algumas adaptações nos itens da resolução e adotará no seu plano de conformidade os seguintes descritivos para as ações de adequação, também visualizados por meio da figura 2:

a) **Objeto:** (O que?) Conterá a ação que deve ser executada para a adequação e conformidade com a Lei nº 13.709/2018, além do número de identificação do controle, o tipo de controle, bem como a representação (em cores) da sua criticidade analisada, seguindo os critérios estabelecidos no mapa de risco;

b) **Prazos**: (Quando?) Serão sugeridos em função da complexidade da adequação e em função do tipo de controle identificado para a referida ação, conforme descrito em 4.1.2;

c) **Ações previstas para reversão da situação identificada**: (Como?) Serão as ações que, após a implementação dos controles, levarão ao alcance do resultado esperado e definido no planejamento;

d) **Critérios de acompanhamento**: (Quem?) O Sistema de Gestão Estratégica da Aeronáutica (GPAer), através do Módulo Plano de Ação, será a ferramenta de suporte ao monitoramento, que contará com os encarregados de coordenação da área responsável, que indicarão os designados para apoiarem na adequação e na atualização dos indicadores do processo;

e) **Trajetória de alcance dos resultados esperados**: (Como?) A cada trimestre deverá ser realizado o registro de ocorrência e atualização dos indicadores no GPAer, para que seja observado no nível estratégico o acompanhamento e o cumprimento dos prazos previstos em cada processo de adequação;

f) **Descrição do controle**: (Por que?) Observações sobre o controle em si, ou seja, detalhamento das informações contidas no controle, de maneira a esclarecer por que e quais são as ações que a área responsável deverá realizar para o cumprimento com as diretrizes da Lei nº 13.709/2018;

g) **Referência**: (Onde?) É o referencial legal/normativo que justifica o controle proposto pela empresa de consultoria, ou seja, onde está o embasamento legal para a respectiva ação, além de contar também com a origem do controle, quando a informação apresentada fizer referência a tabela 2; e

h) ***Gap* associado**: (Quanto?) Observando pela ótica reputacional para o COMAER, os *Gaps* representam as lacunas encontradas e associadas ao processo.

4.2.3 Em sua resolução a ANPD diz ainda que caberá aos agentes de tratamento comprovarem o atendimento ao resultado esperado, além das medidas adotadas para reversão da situação dentro do prazo estabelecido.

4.2.4 Para apoiar nesse processo, os designados para a operação do GPAer deverão entrar em contato com o EMAER por meio do canal <_gpaer.emaer@fab.mil.br>, informando no campo assunto: “Plano de Ação para a LGPD – PCA 16-14”, além de deixar um número para contato telefônico com a finalidade de receberem orientações sobre como proceder no acompanhamento do módulo do plano de ação do referido sistema.

Nº DO CONTROLE Risco alto	**Ação que deve ser executada.**	
	Tipo de Controle: conforme 4.1.2	**Prazo: Sugerido pelo EMAER**
Descrição do controle	Observações sobre o controle.	
Resultado esperado	Ações que levarão ao alcance do resultado esperado.	
Referências	Base legal que justifica o controle proposto.	
Gap associado	Lacunas encontradas e associadas ao processo.	

Figura 2 – Modelo de apresentação gráfica das ações diagnosticadas.

5 PLANO DE AÇÃO

Após a realização do diagnóstico sobre os macroprocessos, serão apresentados a seguir os controles propostos para que o COMAER entre em conformidade com os requisitos da Lei nº 13.709/2018, Lei Geral de Proteção de Dados – LGPD, observando que tais controles representam um trabalho inicial que não esgotam a necessidade por análises mais detalhadas nos setores. Assim, os controles apresentados, bem como a metodologia entregue nos itens anteriores, servirão de modelo para os próximos processos a serem adequados em cada ODGSA.

5.1 ASOCEA

01 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados para capacitação, credenciamento e realização das inspeções nos provedores de serviços de navegação aérea.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados nos processos internos, não só no âmbito do sistema utilizado para esta finalidade, o Sistema Vigilante, mas também nos registros armazenados nos servidores de arquivos da ASOCEA, inclusive daqueles que não foram aprovados no processo seletivo de INSPCEA. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Implantar os critérios de temporalidade aplicados aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 48.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

02 **Risco alto**	**Implementar aviso de privacidade na Ficha de Cadastro para o Curso de Inspeção de Segurança Operacional do Controle do Espaço Aéreo.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário de cadastro para o curso de inspeção de segurança para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar aviso de privacidade na Ficha de Cadastro para o Curso de Inspeção de Segurança Operacional do Controle do Espaço Aéreo.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 48.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

03 **Risco médio**	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos auditados/responsáveis pelas Estações Prestadoras de Serviços de Telecomunicações e Tráfego Aéreo (EPTA).**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Para uma EPTA ser credenciada para realizar sua operação, os responsáveis serão submetidos a critérios definidos pelo COMAER. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados para o credenciamento/auditoria e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.2 ASPAER

04 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante as atividades de relacionamento com os poderes executivo, legislativo e judiciário.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, inclusive os registros armazenados em banco de dados com as informações pessoais daqueles que participarão de agendas oficiais. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Implantar os critérios de temporalidade aplicados aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 45.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

05 **Risco baixo**	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos contatos que possuem relacionamento com o COMAER.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Para o desempenho das suas atribuições a ASPAER necessita possuir contatos institucionais para a concretização da sua missão. Com isso, é recomendável que as informações sejam tratadas em uma base de dados centralizada. Além disso, sempre que possível, para o procedimento de coleta deverão ser apresentadas a finalidade e a temporalidade para a realização do tratamento dos dados coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais dos contatos institucionais e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.3 CECOMSAER

06 **Risco alto**	**Convém que a organização colete o consentimento dos titulares que compõem ou venham a compor o banco de dados dos Jornalistas no Sistema Atena.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Recomenda-se que seja definido um procedimento de coleta do consentimento específico do titular para esse fim e que, no caso dos jornalistas que hoje compõem o banco de dados utilizado pela FAB, seja realizado uma atividade de coleta de consentimento dos mesmos, pois somente de posse deste tipo de formalização se faça uso destes dados. Caso não seja possível a coleta deste tipo de autorização é recomendável a exclusão definitiva das informações desses titulares. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Implementar procedimento de coleta de consentimento dos titulares que façam parte do banco de dados.	
Referências	1) Art. 7º, I e Art. 8º da Lei nº 13.709/2018. 2) RTD nº 17.	
Gap associado	Ausência de mecanismos de consentimento e escolha.	

07 **Risco alto**	**Convém que a organização colete o consentimento dos titulares que compõem ou venham a compor o banco de dados de imagens gerenciadas e divulgadas nas redes sociais do COMAER.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Recomenda-se que seja definido um procedimento de coleta do consentimento específico do titular para esse fim e que, no caso dos militares que hoje compõem o banco de dados utilizado pela FAB, seja realizado uma atividade de coleta de consentimento dos mesmos, pois somente com a posse deste tipo de formalização seja feito o uso destes dados. Caso não seja possível a coleta deste tipo de autorização é recomendável a exclusão definitiva das informações desses titulares, como por exemplo as imagens disponíveis no Flickr.	
Resultado esperado	Implementar procedimento de coleta de consentimento dos titulares que façam parte do banco de dados.	
Referências	1) Art. 7º, I e Art. 8º da Lei nº 13.709/2018.	
Gap associado	Ausência de mecanismos de consentimento e escolha.	

5.4 CENCIAR

08 **Risco alto**	**Restringir o acesso somente aos auditores responsáveis pela auditoria aos documentos recebidos necessários à execução dos trabalhos.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É importante que somente os auditores responsáveis pela auditória tenham acesso aos documentos disponibilizados e também aos documentos gerados durante este processo. Isso garante que somente aqueles auditores designados terão acesso aos materiais daquela auditoria, garantindo assim uma maior segurança contra possíveis acessos indevidos.	
Resultado esperado	Implementar restrição de acesso aos materiais oriundos da auditoria somente ao grupo de trabalho.	
Referências	1) Art. 6, III e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013. 3) RTD nº 25.	
Gap associado	Ausência de Controles de Acesso Lógico.	

09 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a auditoria.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito dos documentos disponibilizados e gerados durante a auditoria, mas também no escopo do sistema utilizado como suporte a este processo, o AUDIFISC. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Implantar os critérios de temporalidade aplicados aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 25.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

10 Risco médio	Convém que seja estabelecido um protocolo para envio de documentações pelos auditados.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Foi identificado que quando se fizer necessário que as unidades auditadas enviem informações para o auditor, estas podem ser enviadas utilizando-se de diversos mecanismos, como armazenamento em repositório FTP ou e-mail. Diante disso convém que seja estabelecido um protocolo único a ser utilizado na comunicação com todas as unidades auditadas em relação ao procedimento de envio destes dados. Isso, além de garantir a segurança e proteção dos dados de acessos indevidos também facilitará a gestão destas informações.	
Resultado esperado	Estabelecer e implantar protocolo para envio de documentações durante a auditoria.	
Referências	1) ABNT NBR ISO/IEC 27002:2013. 2) RTD nº 25.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.5 CENIPA

11 Risco alto	É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a investigação das ocorrências aeronáuticas.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito documentos físicos coletados durante a investigação, mas também no escopo dos sistemas utilizados para esta finalidade, como o DÉDALO. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Implantar os critérios de temporalidade aplicados aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 12.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

12 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante as ações de prevenção de ocorrências aeronáuticas.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito documentos físicos fornecidos durante os cursos presenciais de formação, mas também no escopo dos sistemas utilizados para esta finalidade, como o Cenipa Virtual. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Implantar critérios de temporalidade aplicados aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 13.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

13 Risco alto	**Implementar aviso de privacidade na Ficha de Inscrição dos Cursos oferecidos pelo CENIPA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É recomendável que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha de Inscrição utilizada pelo CENIPA para cadastro aos cursos presenciais e/ou remotos para que os titulares ao preencherem esta ficha estejam cientes de como seus dados pessoais serão tratados apenas durante este processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade na Ficha de Inscrição dos Cursos.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 13.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

14 Risco alto	Revisar o normativo que estabelece protocolos, responsabilidades e atribuições referentes às investigações de acidente aeronáutico.	
	Controle: NORMATIVO	Prazo: 30/JUN/22
Descrição do controle	A NSCA 3-6/2013 tem como objetivo estabelecer protocolos, responsabilidades e atribuições referentes às investigações de acidente aeronáutico, incidente aeronáutico grave e ocorrência de solo com aeronaves militares, realizadas no âmbito do Sistema de Investigação e Prevenção de Acidentes Aeronáuticos (SIPAER). Desta forma se faz necessário a revisão de tal documento para que as orientações sobre o tratamento de dados realizado durante este processo estejam ajustadas aos ditames da LGPD.	
Resultado esperado	Adequar a instrução normativa aos princípios e ditames da Lei nº 13.709/2018.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018. 2) RTD nº 12.	
Gap associado	Ausência de medidas de responsabilização.	

15 Risco médio	Revisar o normativo que estabelece os procedimentos acerca dos programas de Formação e Capacitação do CENIPA.	
	Controle: NORMATIVO	Prazo: 30/JUN/22
Descrição do controle	A NSCA 3-10/2017 tem como objetivo estabelecer procedimentos e definir os programas de Formação e Capacitação dos Recursos Humanos do Sistema de Investigação e Prevenção de Acidentes Aeronáuticos (SIPAER), visando contribuir para a qualidade da formação desenvolvida pelos órgãos constitutivos do Sistema. Desta forma se faz necessário a revisão de tal documento para que as orientações sobre os procedimentos a serem implementados acerca do tratamento de dados realizado durante a execução destes programas estejam ajustadas aos ditames da LGPD.	
Resultado esperado	Adequar a instrução normativa aos princípios e ditames da Lei nº 13.709/2018.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018. 2) RTD nº 13.	
Gap associado	Ausência de medidas de responsabilização.	

16 Risco médio	**Estabelecer instrumento legal junto as instituições homologadas para adequação do relacionamento à LGPD.**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	O CENIPA poderá homologar instituições no âmbito do Ministério da Defesa (MD) ou instituições de ensino superior que tenham curso de Ciências Aeronáuticas ou de Tecnólogo em Aviação Civil, reconhecido pelo Ministério da Educação, para a execução de Curso de Prevenção de Acidentes Aeronáuticos (CPAA). Ao final destes cursos o CENIPA recebe todos os dados pessoais dos alunos concludentes. Neste sentido é recomendável que seja estabelecido instrumento legal onde sejam definidos papéis e responsabilidades das partes quanto à garantia da segurança e proteção dos dados pessoais por eles tratados durante a execução destes cursos.	
Resultado esperado	Estabelecer instrumento Legal entre o CENIPA e as instituições de ensino homologadas.	
Referências	1) Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 13.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

17 Risco médio	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos titulares (externos ao COMAER) que participam dos cursos ofertados pelo CENIPA.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Para um cidadão estar em condições de solicitar matrícula em um dos cursos ofertados pelo CENIPA, deverá seguir alguns critérios definidos pelo COMAER. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados dos participantes externos ao COMAER nos cursos e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.6 CIAER

18 **Risco alto**	**Revisar o Formulário Individual de Dados para Credenciamento (FIDC) utilizado para concessão de credenciais de segurança.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Durante o processo de credenciamento de segurança para pessoas naturais se faz necessário o preenchimento do Formulário Individual de Dados para Credenciamento (FIDC) onde o interessado fornece diversas informações pessoais (suas e de terceiros) para que possa ser investigado e posteriormente concedida tal credencial. Como neste documento o titular consente com o tratamento de seus dados pessoais, é importante que este documento seja ajustado para atender também os requisitos legais apresentados na LGPD, do que se espera de um documento que formalize o consentimento específico do titular para esse fim segundo Art. 7º e 8º da LGPD.	
Resultado esperado	Revisar o Formulário Individual para a adequação aos princípios e ditames da Lei nº 13.709/2018.	
Referências	1) Art. 7º, I e Art. 8º da Lei nº 13.709/2018. 2) RTD nº 11.	
Gap associado	Ausência de mecanismos de consentimento e escolha.	

19 **Risco médio**	**Revisar o Termo de Compromisso de Manutenção de Sigilo (TCMS).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Quando se fizer necessário que pessoa natural que não possua credencial de segurança necessitar realizar o tratamento de informações classificadas em qualquer grau de sigilo, dentre elas possivelmente informações pessoais de terceiros, se fará necessário o preenchimento de Termo de Compromisso de Manutenção de Sigilo (TCMS). É fundamental que tal Termo esteja adequado aos requisitos legais de proteção de dados pessoais nos moldes da LGPD.	
Resultado esperado	Revisar o Termo de Compromisso para a adequação aos princípios e ditames da Lei nº 13.709/2018.	
Referências	1) Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 11.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

20 Risco médio	Revisar o normativo que orienta o credenciamento de segurança.	
	Controle: NORMATIVO	Prazo: 30/JUN/22
Descrição do controle	A ICA 200-13/2017 tem como objetivo disciplinar o processo de credenciamento de segurança de pessoas naturais para o tratamento de informações classificadas. Desta forma, se faz necessária a revisão de tal documento, para que as orientações sobre esse tratamento de dados estejam ajustadas aos ditames da LGPD.	
Resultado esperado	Adequar a instrução normativa aos princípios e ditames da Lei nº 13.709/2018.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018. 2) RTD nº 11.	
Gap associado	Ausência de medidas de responsabilização.	

21 Risco alto	Revisar o normativo que regula o acesso e a divulgação de informações sigilosas e o tratamento de informação classificada.	
	Controle: NORMATIVO	Prazo: 30/JUN/22
Descrição do controle	A ICA 205-47/2015 tem como objetivo regular o acesso e a divulgação de informações sigilosas e o tratamento de informação classificada ou sob restrição de acesso, no âmbito do Comando da Aeronáutica. Desta forma se faz necessária a revisão de tal documento para que as Instruções para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS) também considerem os aspectos de proteção de informações pessoais apresentados pela LGPD.	
Resultado esperado	Revisar a instrução normativa de acordo com os requisitos da Lei nº 13.709/2018.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018.	
Gap associado	Ausência de medidas de responsabilização.	

5.7 COMGAP

22 **Risco alto**	**Revisar o normativo que regula o ciclo de vida dos dados pessoais necessários para a comprovação do voo pelo CAN.**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	A ICA 4-1/2014 tem como objetivo regular o transporte de passageiros no sistema do correio aéreo nacional. Contudo, foi identificado que cada organização realiza o ciclo de vida dos dados pessoais para a comprovação do embarque, segundo seu próprios critérios e limitações.	
Resultado esperado	Revisar a instrução normativa de acordo com os requisitos da Lei nº 13.709/2018 e estabelecer um processo padrão para os Postos CAN sobre o ciclo de vida dos dados pessoais coletados.	
Referências	1) Art. 6º, III da Lei nº 13.709/2018.	
Gap associado	Ausência de medidas de responsabilização.	

5.7.1 COMGAP/DTI

23 **Risco alto**	**É necessária a definição e aplicação de política da temporalidade e destinação final aos dados pessoais coletados e armazenados durante o processo de concessão de VPN.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que seja definida uma tabela de temporalidade com a diferenciação do que é uso corrente e uso intermediário e dos prazos de guarda aplicados a cada documento que contenha dados pessoais tratados neste processo, principalmente aqueles que contenham dados pessoais sensíveis, como atestados médicos. Desta forma é necessário que seja definido quanto tempo e o que será feito com os dados pessoais coletados através do termo de responsabilidade, administrados pelos Centros de Computação que fornecem recurso da VPN.	
Resultado esperado	Definir critérios de temporalidade e destinação final a serem aplicados aos dados pessoais coletados.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 02.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

24 Risco alto	**Implementar aviso de privacidade no Termo de Responsabilidade para Usuários de Sistema Criptográficos Remotos (VPN).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É recomendável que seja acrescentado aviso de privacidade (*privacy notice*) no Termo de Responsabilidade para Usuários de Sistema Criptográficos Remotos (VPN) para que os militares que preencherem o termo estejam cientes de como seus dados pessoais serão tratados apenas durante o processo de concessão de VPN, pelos Centros de Computação e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade no Termo de Responsabilidade para Usuários de Sistema Criptográficos Remotos (VPN).	
Referências	1) Art. 6, I e III e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 02.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

25 Risco alto	**Convém que os requisitos relacionados com segurança da informação sejam incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Convém que os requisitos de segurança da informação sejam identificados usando vários métodos, como, requisitos de conformidade oriundos de política e regulamentações, modelos de ameaças, análises críticas de incidentes ou o uso de limiares de vulnerabilidade. Convém também que os resultados da identificação sejam documentados e analisados criticamente por todas as partes interessadas. Além disso, é importante que os controles e requisitos de segurança da informação reflitam o valor da informação envolvida para o negócio e o seu potencial impacto negativo, que possa resultar de uma falha da segurança da informação.	
Resultado esperado	Aplicar as diretrizes para aquisição ou desenvolvimento de sistemas de informação, atualizado com a necessidade de atendimento aos requisitos de segurança da informação.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 14.2.1). 3) Norma Complementar nº 16 DSIC/GSIPR. 4) RTD nº 01, 55 e 56.	
Gap associado	Ausência de mecanismos de desenvolvimento seguro.	

26 Risco médio	**Convém que regras para o desenvolvimento seguro de sistemas e software sejam estabelecidas e aplicadas aos desenvolvimentos realizados dentro da organização.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Convém que políticas para o projeto e o desenvolvimento de sistemas incluam diretrizes para as necessidades de tratamento de dados pessoais da organização baseado nos conceitos de *Privacy by Design* e *Privacy by Default,* bem como nas obrigações dos titulares e nos tipos de tratamentos realizados pela organização. Os elos do STI possuem o Guia para o Desenvolvimento e Manutenção de Produtos de Software por meio do Método Ágil como orientador, mas é importante que seja estabelecido um método único que considere os desenvolvimentos ágeis e não ágeis e que todos se baseiem nas boas práticas do desenvolvimento seguro.	
Resultado esperado	Implementar o processo de desenvolvimento de aplicações com as regras de privacidade de dados aplicável a todas as unidades que realizam o desenvolvimento de sistemas e softwares.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 14.2.1). 3) Norma Complementar nº 16 DSIC/GSIPR. 4) RTD nº 01, 55 e 56.	
Gap associado	Ausência de mecanismos de desenvolvimento seguro.	

27 Risco alto	**Convém que os sistemas de informação da FAB sejam analisados criticamente, a intervalos regulares, para verificar a conformidade com as normas e políticas de segurança da informação da organização.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Convém que a verificação de conformidade técnica seja analisada criticamente, preferencialmente com o apoio de uma ferramenta automática, a qual gera relatórios técnicos para a interpretação dos especialistas técnicos. Alternativamente, análises críticas manuais (auxiliado por ferramentas de software apropriadas, se necessário) pode ser realizada por meio de questionários (Avaliação de Riscos de Sistemas) que avaliem a presença/ausência das práticas de segurança da informação. Análise de conformidade também engloba, por exemplo, testes de invasão e avaliações de vulnerabilidades, que podem ser realizadas por peritos independentes contratados especificamente para esta finalidade. Isto pode ser útil na detecção de vulnerabilidades no sistema e na verificação do quanto os controles são eficientes na prevenção de acessos não autorizados devido a estas vulnerabilidades.	
Resultado esperado	Aplicar procedimentos de avaliação crítica dos sistemas de informação do COMAER para identificação de conformidade técnica estabelecido e implementado periodicamente.	
Referências	1) ABNT NBR ISO/IEC 27701 (Item 6.15.2.3).	
Gap associado	Ausência de mecanismos para garantir a segurança *web*.	

28 Risco alto	Convém que seja desenvolvida e implementada uma política para o uso de controles criptográficos para a proteção da informação.	
	Controle: TECNOLÓGICO	Prazo: 14/DEZ/23
Descrição do controle	Convém que o COMAER estabeleça uma política para uso de controles criptográficos que identifique os controles adequados para atender os objetivos da Política de Segurança da Informação e que forneça informações para os titulares em relação às circunstâncias em que utiliza a criptografia para proteger os dados pessoais tratados.	
Resultado esperado	Implementar política de uso de controles criptográficos.	
Referências	1) Art. 18, IV da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 6.7.1.1).	
Gap associado	Ausência de controles criptográficos.	

29 Risco alto	Habilitar os mecanismos de rastreabilidade no Portal do Militar.	
	Controle: TECNOLÓGICO	Prazo: 14/DEZ/23
Descrição do controle	De acordo com as boas práticas de segurança da informação, é recomendável que os sistemas registrem a identificação, o endereço IP e as ações executadas pelos usuários, bem como data e hora dos eventos, a fim de que seja possível rastrear os logs, aumentando a segurança dos dados pessoais tramitados nos sistemas e permitindo garantir também que possíveis violações de dados sejam facilmente rastreadas. Uma vez que foi identificado que os operadores das Organizações Militares podem acessar o contracheque dos militares, documento este que comprova o depósito dos vencimentos de um funcionário em sua conta bancária, é recomendável que no Portal do Militar, minimamente no que se refere à consulta aos contracheques (por exemplo), sejam implementados mecanismos de rastreabilidade de maneira a garantir a identificação durante uma eventual investigação.	
Resultado esperado	Implementar mecanismos de rastreabilidade no Portal do Militar.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 12.4.1).	
Gap associado	Ausência de mecanismos de registro de Eventos, Rastreabilidade e Salvaguarda de Logs.	

30 **Risco alto**	**É recomendável que o COMAER elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o Sistema Integrado de Logística de Material e de Serviços (SILOMS).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nessa Lei. Desta forma, mesmo que de maneira proativa, é recomendável que o COMAER elabore tal relatório para o SILOMS para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistema da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível de riscos. Um exemplo potencial de não conformidade com a divulgação de dados pessoais pode ser observado na solução prévia do e-PAG.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 29134:2020.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

31 **Risco baixo**	**Convém que seja avaliada a utilização de solução que permita descobrir e governar os dados pessoais.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Como a FAB necessita cada vez mais realizar uma melhor gestão sobre os dados por ela tratados é importante que seja implementada solução que permita gerenciar os dados em um único local, realizando a descoberta destes dados em diferentes repositórios (estruturados ou não) e executando processos para garantir a qualidade dos dados, de modo que eles tenham seu ciclo de vida considerados.	
Resultado esperado	Avaliar a implantação de uma solução de Gerenciamento ou de Descoberta de Dados (*Master Data Management – MDM e/ou Data Discovery*) em apoio a LGPD.	
Referências	1) Art. 6º, V da Lei nº 13.709/2018.	
Gap associado	Ausência de mecanismos para garantir a precisão e a qualidade.	

32 Risco alto	**Deverá desenvolver ou adquirir um sistema para realizar o gerenciamento unificado de dados pessoais não estruturados, à luz da LGPD, de todas aquelas pessoas que se relacionam com o COMAER e não possuem seus dados no SIGPES ou SIGEPE.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Em função do processo de adequação à LGPD foram observadas várias demandas por tratamento de dados pessoais que poderiam ser administrados por um único sistema. Esses dados são referentes aquelas pessoas que NÃO são militares ou servidores civis do COMAER, que já possuem suas informações administradas pelo SIGPES ou SIGEPE. Tal solicitação foi encaminhada à DTI por ocasião do planejamento do PDTI 22-25, porém o EMAER necessita do posicionamento técnico da Diretoria para a coordenação com os demais ODSA para o aprimoramento da lista de requisitos. Para a adequação dessa ação deverão ser consideradas as seguintes ações: **03, 05, 06, 17, 54, 58, 61, 72, 83, 94, 95, 96, 112, 116 e 121.**	
Resultado esperado	Implantar, até o final do prazo, um sistema que reúna tais informações não estruturadas (requisitos especificados no PDTI), possibilitando entregar aos titulares a gestão de suas próprias informações, conforme preconiza a Lei.	
Referências	1) Art. 5º, 6º, 49 e 50 da Lei nº 13.709/2018.	
Gap associado	Ausência de mecanismos para garantir a precisão e a qualidade.	

5.7.2 COMGAP/DTI/CCA-BR

33 Risco médio	**Revisar o normativo que orienta as Organizações do COMAER quanto aos princípios de segurança da informação que devem ser seguidos.**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	A NSCA 7-13/2013 tem como objetivo orientar as Organizações do COMAER quanto aos princípios de segurança da informação que devem ser seguidos a fim de garantir a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações armazenadas, processadas ou em trânsito a fim de garantir a Defesa do Escopo Cibernético do Comando da Aeronáutica. Desta forma se faz necessário a revisão de tal documento para que as orientações passadas às organizações através das diversas políticas contidas neste documento estejam ajustadas às atualizações de segurança identificadas nos últimos anos, assim como aos ditames da LGPD.	
Resultado esperado	Atualizar e divulgar o Regulamento de Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018. 2) RTD nº 03.	
Gap associado	Ausência de medidas de responsabilização.	

34 **Risco alto**	**Convém que todos os militares que realizem o tratamento de dados pessoais no sistema SIGAER devem receber treinamento, educação e conscientização apropriados, e as atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Convém que medidas sejam implementadas para assegurar que membros que tenham acesso à dados pessoais no sistema SIGAER estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano reputacional ou da marca), para os membros da organização (por exemplo, consequências disciplinares) e para o titular (por exemplo, consequências físicas, materiais e emocionais) da violação de privacidade ou de regras de segurança e procedimentos, especialmente aqueles relacionados ao manuseio de dados pessoais.	
Resultado esperado	Implementar o programa de conscientização.	
Referências	1) Art. 50, I, “a)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.2.2). 3) RTD nº 04.	
Gap associado	Ausência de mecanismos de conscientização sobre a importância da Privacidade e da Segurança da Informação.	

35 **Risco alto**	**É recomendável a implementação de medidas técnicas e organizacionais que garantam o tratamento apenas dos dados essenciais ao objetivo dos processos do SIGAER.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Uma vez que durante a execução deste processo existe acesso a informações pessoais e sensíveis, sendo estas coletadas em diversas fontes, é recomendável que sejam implementadas medidas de segurança, desde o momento da criação dos processos de carga de dados, incluindo também medidas para a anonimização daqueles dados que identificam seus proprietários e não sejam fundamentais para que os usuários do Sistema de Apoio à Decisão realizem suas consultas e relatórios.	
Resultado esperado	Implementar medidas avançadas de segurança.	
Referências	1) Art. 6º, III da Lei nº 13.709/2018. 2) RTD nº 04.	
Gap associado	Ausência de medidas para assegurar a Limitação da Coleta.	

36 **Risco alto**	**Habilitar os mecanismos de rastreabilidade do SIGAER.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	De acordo com as boas práticas de segurança da informação, é recomendável que os sistemas registrem a identificação, o endereço IP e as ações executadas pelos usuários, bem como data e hora dos eventos, a fim de que seja possível rastrear os *logs*, aumentando a segurança dos dados pessoais tramitados nos sistemas e permitindo garantir também que possíveis violações de dados sejam facilmente rastreadas. Desta forma é recomendável que o SIGAER possua mecanismos de rastreabilidade de maneira a garantir a identificação durante uma eventual investigação.	
Resultado esperado	Implementar mecanismos de rastreabilidade no Sistema de Apoio à Decisão.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 12.4.1). 3) RTD nº 04.	
Gap associado	Ausência de mecanismos de registro de Eventos, Rastreabilidade e Salvaguarda de *Logs*.	

37 **Risco alto**	**Habilitar os mecanismos de rastreabilidade do SAM.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	De acordo com as boas práticas de segurança da informação, é recomendável que os sistemas registrem a identificação, o endereço IP e as ações executadas pelos usuários, bem como data e hora dos eventos, a fim de que seja possível rastrear os logs, aumentando a segurança dos dados pessoais tramitados nos sistemas e permitindo garantir também que possíveis violações de dados sejam facilmente rastreadas. Desta forma é recomendável que o SAM possua mecanismos de rastreabilidade de maneira a garantir a identificação durante uma eventual investigação. O CCA-BR deverá auxiliar a CPO na ação 75.	
Resultado esperado	Implementar mecanismos de rastreabilidade no Sistema de Apoio à Decisão.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 12.4.1). 3) RTD nº 55.	
Gap associado	Ausência de mecanismos de registro de Eventos, Rastreabilidade e Salvaguarda de *Logs*.	

5.7.3 COMGAP/DTI/CCA-RJ

38 **Risco médio**	**Revisar o contrato com a empresa que presta serviço de fábrica de softwares para a Força Aérea Brasileira.**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	Uma vez que a FAB, ou pelo menos o CCA-RJ, utiliza os serviços de uma empresa especializada em desenvolvimento e manutenção de sistemas da FAB (no caso do CCA-RJ a empresa Plenos) e que seus funcionários têm acesso, pela natureza de suas atividades, a inúmeros dados pessoais e confidenciais durante a realização de suas atividades, é necessário que este contrato seja revisto para que o mesmo possua todas as cláusulas referentes à atividade de operador realizada pela empresa segundo a LGPD.	
Resultado esperado	Revisar e adequar o contrato com a LGPD.	
Referências	1) Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 01.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

39 **Risco alto**	**É recomendável que o COMAER elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o Sistema de Informações Gerenciais de Pessoal (SIGPES).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nessa Lei. Desta forma, mesmo que de maneira proativa, é recomendável que o COMAER elabore tal relatório para o SIGPES para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistema da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível de riscos.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 29134:2020.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.7.4 COMGAP/DTI/CCA-SJ

40 **Risco alto**	**É recomendável que o COMAER elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o Sistema Informatizado de Gestão Arquivística de Documentos da Aeronáutica (SIGADAER).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nessa Lei. Desta forma, mesmo que de maneira proativa, é recomendável que o COMAER elabore tal relatório para o SIGADAER (ou outro sistema que vier a substituí-lo) para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistema da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível de riscos.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 29134:2020.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.8 COMGEP

41 **Risco alto**	**É recomendável que o COMAER elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o Sistema de Informações Gerenciais de Pessoal (SIGPES).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nessa Lei. Desta forma, mesmo que de maneira proativa, é recomendável que o COMAER elabore tal relatório para o SIGPES para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistema da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível de riscos.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 29134:2020.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

42 Risco alto	É recomendável que o COMAER elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o Sistema Informatizado de Gestão Arquivística de Documentos da Aeronáutica (SIGADAER).	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nessa Lei. Desta forma, mesmo que de maneira proativa, é recomendável que o COMAER elabore tal relatório para o SIGADAER (ou outro sistema que vier a substituí-lo) para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistema da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível de riscos.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 29134:2020.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

43 Risco médio	Implementar aviso de privacidade no Formulário de Proposta de Prestação de Tarefa por Tempo Certo.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no Formulário de Proposta de Prestação de Tarefa por Tempo Certo para que os titulares que preencherem tal documento estejam cientes de como seus dados pessoais serão tratados e de que serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade no Formulário de Proposta de Prestação de Tarefa por Tempo Certo.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 54.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

44 Risco alto	**Definir e apresentar a finalidade do tratamento dos dados pessoais coletados no Sistema de Informações Gerenciais de Pessoal (SIGPES).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	As organizações devem comunicar aos titulares dos dados pessoais a finalidade para a qual serão coletadas e como serão processadas. Essa comunicação deve ocorrer antecipadamente ao momento da coleta dos dados. Desta forma, é importante que seja acrescentado aviso de privacidade (*privacy notice*) ao módulo de cadastro/consulta de informações pessoais para que os titulares tenham ciência de como o COMAER tratará e garantirá a segurança dos dados a ela fornecidos no SIGPES ou Portal do Militar.	
Resultado esperado	Implantar os Avisos de Privacidade no SIGPES e no Portal do Militar.	
Referências	1) Art. 6º, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

45 Risco baixo	**Convém que seja desenvolvido um Repositório Arquivístico Digital Confiável (RDC-Arq).**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Uma vez que há um número cada vez maior de documentos que contém informações pessoais sendo tratados digitalmente é importante que a FAB desenvolva e implemente um repositório digital que armazena e gerencia esses documentos, seja nas fases corrente e intermediária, seja na fase permanente. E que seja capaz de manter autênticos os materiais digitais, de preservá-los e prover acesso a eles pelo tempo necessário.	
Resultado esperado	Implantar os Repositório Arquivístico Digital Confiável (RDC-Arq).	
Referências	1) Art. 6º, V da Lei nº 13.709/20.	
Gap associado	Ausência de mecanismos para garantir a precisão e a qualidade.	

5.8.1 COMGEP/CDA

46 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a aplicação do teste de avaliação do condicionamento físico para exames de admissão e de seleção.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito dos documentos físicos coletados e gerados durante a realização dos exames, mas também no escopo do sistema utilizado para esta finalidade. Com atenção especial para os dados pessoais dos candidatos não aprovados. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 09.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

47 **Risco alto**	**Implementar aviso de privacidade nas Fichas de Anamnese.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha de Anamnese e de Avaliação do TACF para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade na Ficha Individual.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 10.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.8.2 COMGEP/CENDOC

48 **Risco baixo**	**É recomendável a implementação de um processo de registro das solicitações de consulta aos documentos no arquivo temporário.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	A consulta e utilização, sob qualquer forma, da documentação armazenada no arquivo temporário pode ser realizada de diversas formas, dentre elas diretamente na sede do Arquivo Intermediário ou sob forma de empréstimo, por exemplo. Desta forma, é recomendável a criação de um mecanismo de registro centralizado e que, independentemente de como ocorrer esta consulta, o CENDOC tenha mecanismos de rastreabilidade, inclusive nesta etapa do processamento realizado.	
Resultado esperado	Criar e implementar um mecanismo de registro de consultas aos documentos sob a gestão do arquivo intermediário.	
Referências	1) Art. 6º, V da Lei nº 13.709/20. 2) RTD nº 30.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

49 **Risco médio**	**Implementar a proteção contra ameaças externas e do meio ambiente nas dependências do Arquivo Intermediário.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Considerando que boa parte dos documentos sob a gestão do Arquivo Intermediário estão aguardando sua destinação final (eliminação ou guarda permanente), seja em razão do final de sua vigência, dos longos prazos de prescrição, precaução ou por serem raramente consultados, se faz necessário que sejam projetadas e aplicadas camadas de proteção física em seu ambiente de modo a prevenir desastres naturais, ataques maliciosos ou acidentes na estrutura do Arquivo Intermediário.	
Resultado esperado	Implementar controles ambientais no Arquivo Intermediário.	
Referências	1) ABNT NBR ISO/IEC 27701 (Item 11.1.4). 2) RTD nº 30.	
Gap associado	Ausência de Controles de Segurança em Redes, Proteção Física e do Ambiente.	

50 **Risco baixo**	**Convém que o sistema de classificação da informação da FAB considere explicitamente Dados Pessoais como parte do Plano de Classificação de Documentos de Arquivo.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É importante que os dados pessoais sejam considerados em todo o Plano de Classificação de Documentos de Arquivo para que seja possível entender qual tipo de dado pessoal é tratado pela FAB, onde estes dados pessoais estão armazenados e os sistemas pelos quais ele pode fluir, especialmente no que se refere a temporalidade e ao término do tratamento de dados. Será muito importante caso o CENDOC possa contribuir para o desenvolvimento das seguintes ações: **01, 04, 09, 11, 12, 23, 46, 52, 55, 56, 62, 65, 67, 69, 71, 74, 78, 80, 82, 85, 86, 89, 106, 107, 109, 114, 117, 118, 122, 125, 127 e 128**.	
Resultado esperado	Revisar o plano de Classificação de Documentos de Arquivo.	
Referências	1) Art. 15 e 16 da Lei nº 13.709/20. 2) RTD nº 30 e 31.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

51 **Risco médio**	**Implementar a proteção contra ameaças externas e do meio ambiente nas dependências do Arquivo Permanente.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Considerando que os documentos sob a gestão do Arquivo Permanente estão lá para garantir a preservação do patrimônio documental de interesse histórico, cultural e social da FAB, se faz necessário que sejam projetadas e aplicadas camadas de proteção física em seu ambiente de modo a prevenir desastres naturais ataques maliciosos ou acidentes na estrutura do Arquivo Permanente.	
Resultado esperado	Implementar controles ambientais no Arquivo Permanente.	
Referências	1) Art. 15 e 16 da Lei nº 13.709/20. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.4). 3) RTD nº 31.	
Gap associado	Ausência de Controles de Segurança em Redes, Proteção Física e do Ambiente.	

5.8.3 COMGEP/DIRAP

52 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante os processos seletivos realizados nos Serviços de Recrutamento e Preparo de Pessoal da Aeronáutica (SEREP).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados durante a realização dos processos seletivos, não só no âmbito dos documentos físicos fornecidos durante os exames de admissão e seleção, mas também no escopo dos sistemas utilizados pelas instituições. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER. Observar que tal política deverá constar ou refletir nos editais ou sumários contendo orientações e critérios de seleção, especialmente no momento da coleta dos dados, por ocasião dos processos seletivos.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 6º - III, Art. 11, Art. 15 - I e II, Art. 40 e 46 da Lei nº 13.709/2018. 2) RTD nº 15.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

53 **Risco alto**	**Implementar aviso de privacidade no Formulário de Solicitação de Inscrição nos processos seletivos realizados nos Serviços de Recrutamento e Preparo de Pessoal da Aeronáutica (SEREP).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É recomendável que seja acrescentado aviso de privacidade (*privacy notice*) no Formulário de Solicitação de Inscrição utilizado pelas instituições de ensino para a realização dos exames de admissão e seleção, com o objetivo de informar aos titulares no momento do preenchimento da ficha para que estejam cientes de como seus dados pessoais serão tratados durante processo seletivo. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implantar o aviso de privacidade no Formulário de Solicitação de Inscrição.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 15.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

54 Risco médio	**É recomendável que seja definido um procedimento padrão para o tratamento dos formulários gerados pela solicitação de inscrição e que não são aproveitadas para inserção no SIGPES.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Ao ocorrerem os processos seletivos conduzidos nos SEREP, todos os dados pessoais dos candidatos aprovados são transferidos para o SIGPES, contudo, para os candidatos não aprovados o mesmo não ocorre, sendo necessário incluir esses dados pessoais em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade de coleta. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados durante os processos de seleção e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar as informações dos candidatos não selecionados.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 15.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

55 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante o processo de emissão/renovação das Carteiras de Identidade Militar ou dos Cartões Militar de Identificação.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito dos documentos físicos fornecidos durante o ciclo de coleta, mas também no escopo dos sistemas utilizados pela organização. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

5.8.4 COMGEP/DIRENS

56 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante os processos seletivos.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados durante a realização dos processos seletivos, não só no âmbito dos documentos físicos fornecidos durante os exames de admissão e seleção, mas também no escopo dos sistemas utilizados pelas instituições de ensino, como o SIGC e o SGCEM. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER. Observar que tal política deverá constar ou refletir nos editais, especialmente no momento da coleta dos dados, por ocasião dos processos seletivos.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 6º - III, Art. 11, Art. 15 - I e II, Art. 40 e 46 da Lei nº 13.709/2018. 2) RTD nº 15.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

57 **Risco alto**	**Implementar aviso de privacidade no Formulário de Solicitação de Inscrição (FSI).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É recomendável que seja acrescentado aviso de privacidade (*privacy notice*) no Formulário de Solicitação de Inscrição utilizado pelas instituições de ensino para a realização dos exames de admissão e seleção, com o objetivo de informar aos titulares no momento do preenchimento da ficha para que estejam cientes de como seus dados pessoais serão tratados durante processo seletivo. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implantar o aviso de privacidade no Formulário de Solicitação de Inscrição.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 15.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

58 Risco alto	**É recomendável que seja definido um procedimento padrão para o tratamento dos formulários gerados pela solicitação de inscrição e que não são aproveitadas para inserção no SIGPES.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Ao ocorrerem os processos seletivos, todos os dados pessoais dos candidatos aprovados nos diversos concursos de admissão são transferidos para o SIGPES, contudo, para os candidatos não aprovados o mesmo não ocorre, sendo necessário incluir esses dados pessoais em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade de coleta. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados durante os processos de seleção e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar as informações dos candidatos não selecionados.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 15.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

59 Risco alto	**Convém que o COMAER realize uma avaliação completa de segurança no Sistema de Gerenciamento e Controle de Exames Militares (SGCEN).**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	De acordo com a avaliação de riscos realizada no sistema SGCEN foi identificado que o mesmo não contempla as melhores práticas de segurança e privacidade, gerando assim um alto risco aos dados por ele tratados. Desta forma, é recomendável que, utilizando como base o Relatório de Risco dos Sistemas da Informação da FAB, seja avaliado de forma mais aprofundada as fragilidades de segurança do sistema e que sejam avaliados os próximos passos do desenvolvimento do sistema ou até mesmo a sua substituição. A DIRENS deverá solicitar o apoio da DTI para a referida avaliação.	
Resultado esperado	Implantar, até o final do prazo, as melhorias quanto a segurança e a privacidade dos dados no sistema.	
Referências	1) ABNT NBR ISO/IEC 27701 (Item 5.4.1.2).	
Gap associado	Ausência de mecanismos para garantir a segurança *web*.	

60 **Risco alto**	**Implementar um aviso de privacidade no Formulário de inclusão/recadastramento de alunos das escolas assistenciais do COMAER.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no Formulário de inclusão/recadastramento de alunos das escolas assistenciais para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade no Formulário de inclusão/recadastramento de alunos das escolas assistenciais do COMAER.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

61 **Risco médio**	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos alunos das escolas assistenciais do COMAER.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Os pais que procuram as escolas assistenciais do COMAER para matricularem seus filhos, serão submetidos a critérios de seleção definidos pelas escolas. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados pessoais coletados dos titulares responsáveis, bem como dos dependentes menores (dados pessoais sensíveis). Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados nas escolas assistenciais e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações sensíveis.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 11, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.8.5 COMGEP/DIRSA

62 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais durante o tratamento das solicitações de Guias de Apresentação de Beneficiários e Autorizações de Ressarcimento.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda de cada documento que contenha dados pessoais tratados nesses processos, não só no âmbito do Processo Administrativo de Gestão, mas também no escopo dos sistemas utilizados para esta finalidade, como o SISAUC. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 18.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

63 **Risco alto**	**Implementar aviso de privacidade nos sistemas de atendimento on-line nos hospitais da FAB.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	As unidades hospitalares da FAB disponibilizam, em sua maioria mecanismos de acesso remoto para seus usuários aos serviços de Agendamento de Consulta e Resultado de Exames. É necessário que sejam acrescentados avisos de privacidade (*privacy notice*) nos formulários de acesso a estes serviços para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo para essa finalidade, especialmente por se tratar de dados pessoais e em sua grande maioria sensíveis. (As informações dos hospitais que possibilitam a marcação de consulta podem ser encontradas no seguinte portal: https://www.fab.mil.br/aba_reservainterativa#agendar_consulta) Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item. Para o ambiente interno, no que se refere ao processo de marcação de consultas no Portal do Militar, o “Termo de Consentimento” apresentado não está de acordo com a LGPD, necessitando ser revisado.	
Resultado esperado	Aplicar Avisos de Privacidades nos Formulários de Agendamento de Consulta e Resultado de Exames das unidades hospitalares da FAB.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

64 Risco alto	**Implementar aviso de privacidade no formulário de Solicitação de Encaminhamento à Rede Complementar do SISAU.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário de solicitação de encaminhamento para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implantar o aviso de privacidade no formulário de Solicitação de Encaminhamento.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 18.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

65 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante o tratamento das solicitações de Guias de Apresentação de Beneficiários e Autorizações de Ressarcimento, para os procedimentos realizados no exterior.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar critérios de temporalidade aos documentos/registros utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 19.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

66 Risco alto	**Implementar aviso de privacidade no Formulário para Autorização de Ressarcimento de Despesas em Saúde no exterior.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário de solicitação de autorização para realização de gastos com saúde por militares que estejam em missões no exterior, para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade no Formulário de Solicitação de Autorização para realização de gastos com saúde no exterior.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 19.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

67 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante o julgamento das ações pela Junta Superior de Saúde.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito das atas geradas ao final da análise, mas também no escopo dos registros criados no sistema que dá suporte a este processo, o SAL9000. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 20.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

68 Risco alto	**Implementar um aviso de privacidade na Declaração do Militar/Titular Contribuinte para inclusão/recadastramento de dependentes no Sistema de Saúde da Aeronáutica.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Declaração do Militar Contribuinte para inclusão/recadastramento de dependentes no Sistema de Saúde de Aeronáutica para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade na Declaração do Militar/Titular Contribuinte para inclusão/recadastramento de dependentes no Sistema de Saúde da Aeronáutica.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 21.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.8.6 COMGEP/IPA

69 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a realização dos Exames de Aptidão Psicológica.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito dos documentos físicos coletados e gerados durante a realização dos exames, mas também no escopo do sistema utilizado para esta finalidade, como o SIGCEM. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 27.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

70 Risco alto	Implementar aviso de privacidade na Ficha Individual.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha Individual utilizada pela Divisão de Seleção do IPA durante a realização dos Exames de Aptidão Psicológica para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade na Ficha Individual.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 27.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.9 COMPREP

71 Risco alto	É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante os acessos às instalações da Aeronáutica.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito dos formulários físicos preenchidos durante o acesso, mas também no escopo dos sistemas utilizados para esta finalidade, como os sistemas das Centrais de Visitantes. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 32.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

72 Risco baixo	**É recomendável que seja definido um procedimento padrão para o tratamento dos formulários gerados durante o acesso às instalações da Aeronáutica.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Uma vez que são preenchidos, minimamente duas fichas de controle de entrada/saída, tanto para pedestres quanto para veículos, e estes documentos são encaminhados para o Grupo de Segurança e Defesa (GSD) da unidade ao final do serviço, é recomendável que todos estes grupos tenham um procedimento padrão, bem como sistema, para o tratamento de tais informações a fim de garantir a segurança das informações pessoais aí apresentadas, assim como para não correr o risco de realizar o tratamento após alcançada sua finalidade de coleta. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados durante os acessos às instalações da Aeronáutica e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 32.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

73 Risco baixo	**É recomendável que seja definido um procedimento padrão para o cadastramento e recadastramento de veículos para acessar as instalações da Aeronáutica.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Para que os veículos dos militares que circulam em cada OM tenham seu acesso garantido e facilitado se faz necessário o cadastramento prévio destes veículos com a coleta de diversas informações pessoais do proprietário. Uma vez que não há um padrão de como e onde estas informações serão armazenadas, é recomendável que se crie procedimento padrão, bem como um sistema, para o tratamento de tais informações de modo a ter condições de garantir a segurança dos dados coletados e garantir também o atendimento aos demais requisitos da LGPD.	
Resultado esperado	Padronizar os procedimentos de cadastramento e recadastramento de veículos para acessos às instalações da Aeronáutica.	
Referências	1) Art. 6º, V da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 32.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.10 CPO

74 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a execução da avaliação de desempenho de oficiais e graduados.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo, não só no âmbito do dossiê de avaliação do militar, mas também no escopo dos sistemas utilizados para esta finalidade, como o SISPROM, o SAM e o SAG. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 5 e 6.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

75 **Risco alto**	**Habilitar os mecanismos de rastreabilidade do SISPROM.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	De acordo com as boas práticas de segurança da informação, é recomendável que os sistemas registrem a identificação, o endereço IP e as ações executadas pelos usuários, bem como data e hora dos eventos, a fim de que seja possível rastrear os logs, aumentando a segurança dos dados pessoais tramitados nos sistemas e permitindo garantir também que possíveis violações de dados sejam facilmente rastreadas. Desta forma é recomendável que o SISPROM possua mecanismos de rastreabilidade de maneira a garantir a identificação durante uma eventual investigação. O Sistema de Avaliação de Graduados (SAG) deverá receber a mesma atenção até que seja substituído. O CCA-BR deverá auxiliar a CPO nesta ação.	
Resultado esperado	Implementar Sistema de Registro de Informações de Promoção com mecanismos de rastreabilidade.	
Referências	1) Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013 (item 12.4.1). 3) RTD nº 5 e 6.	
Gap associado	Ausência de mecanismos para garantir a segurança *web*.	

76 Risco alto	**Convém que o COMAER realize uma avaliação completa de segurança nos Sistemas de Avaliação, bem como no Sistema de Análise de Mérito.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	De acordo com a avaliação de riscos realizada no Sistema SAG e no Sistema SAM foi identificado que o mesmo não contempla as melhores práticas de segurança e de privacidade, gerando assim um alto risco aos dados por ele tratados. Desta forma é recomendável que, utilizando como base o Relatório de Risco dos Sistemas da Informação da FAB, seja avaliado de forma mais aprofundada as fragilidades de segurança do sistema e que sejam avaliados os próximos passos do desenvolvimento ou até mesmo da sua substituição. Esse controle deve ser extensivo aos demais sistemas de avaliação A CPO deverá solicitar o apoio da DTI para a referida avaliação.	
Resultado esperado	Avaliar os sistemas quanto à segurança e a privacidade, definindo plano de melhorias para implantação das melhores práticas.	
Referências	1) Art. 6º, V e Art. 46 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 5.4.1.2).	
Gap associado	Ausência de mecanismos para garantir a segurança *web*.	

77 Risco alto	**Restringir ao máximo o acesso (por terceiros) às informações pessoais produzidas no Setor.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É importante que somente a SECPROM e os titulares tenham acesso aos documentos disponibilizados ou gerados pelos processos internos da Comissão. Isso garante que somente aqueles devidamente credenciados terão acesso aos documentos/produtos da CPO, garantindo assim uma maior segurança contra possíveis acessos indevidos.	
Resultado esperado	Implementar mecanismos de restrição de acesso às informações pessoais, especialmente por terceiros, produzidas pelos processos internos da CPO.	
Referências	1) Art. 6, VII e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27002:2013. 3) RTD nº 5 e 6.	
Gap associado	Ausência de Controles de Acesso Lógico.	

5.11 DCTA

78 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a prospecção de oportunidades.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados durante a prospecção em Ciência, Tecnologia e Inovação. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 33.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

79 **Risco alto**	**Implementar aviso de privacidade no Formulário de Estudos Prospectivos.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no Formulário de Estudos Prospectivos, documento que oficializa a solicitação de prospecção de estudos para que os titulares que preenchem tal documento estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o aviso de privacidade no Formulário de Estudos Prospectivos.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 33.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

80 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a formalização de parcerias institucionais.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais coletados tratados durante o estabelecimento e formalização das parcerias para execução de atividades ou projetos conjuntos de Pesquisa, Desenvolvimento e Inovação (P,D&I). Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 34.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

81 **Risco alto**	**Revisar os anexos da NSCA 80-12/2020.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Uma vez que as Instituições Científicas, Tecnológicas e de Inovação (ICT) do Comando da Aeronáutica necessitam estabelecer acordos de parceria com instituições públicas e privadas para realização de atividades conjuntas de pesquisa científica e tecnológica e de desenvolvimento de tecnologia, produto, processo ou serviço é fundamental que este instrumento legal, utilizado para estabelecer tal parceria, seja revisto para que o mesmo possua todas as cláusulas referentes às responsabilidades das partes quanto a manutenção da privacidade dos dados pessoais tratados durante tal relacionamento. Os anexos que necessitam de revisão são o “A” (Acordo de Parceria para Atividades de P,D&I), o “B” (Acordo de Compartilhamento e Gestão da Propriedade Intelectual e Participação nos Resultados), o “C” (Convênio para Projeto de Pesquisa, Desenvolvimento e Inovação), o “D” (Acordo de Cooperação Internacional), o “E” (Termo de Outorga para Pesquisa, Desenvolvimento e Inovação) e o “F” (Contrato de Aquisição de Produtos para Pesquisa, Desenvolvimento e Inovação).	
Resultado esperado	Revisar os anexos da NSCA80-12/2020 à Lei nº 13.709/218.	
Referências	1) Art. 6º - III, Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 34.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

82 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante os processos seletivos do ITA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados durante a realização dos processos seletivos, não só no âmbito dos documentos físicos fornecidos durante os exames de admissão e seleção, mas também no escopo dos sistemas utilizados pela instituição de ensino. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER. Observar que tal política deverá constar ou refletir nos editais, especialmente no momento da coleta dos dados, por ocasião dos processos seletivos.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 6º - III, Art. 11, Art. 15 - I e II, Art. 40 e 46 da Lei nº 13.709/2018. 2) RTD nº 15.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

83 Risco Alto	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos titulares (externos ao COMAER) que participam dos contratos de parceria em pesquisa e desenvolvimento ou dos cursos ofertados pelo ITA.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Para um cidadão estar em condições de solicitar matrícula no ITA ou participar de um termo de parceria de pesquisa e desenvolvimento no DCTA, deverá seguir alguns critérios definidos pelo COMAER. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados dos participantes externos ao COMAER nos cursos do ITA ou parcerias no DCTA e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 11, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.12 DECEA

84 **Risco alto**	**É recomendável que o DECEA elabore um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) para o processo de Solicitar Autorização para Voo de Aeronaves Remotamente Pilotadas.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, o RIPD deverá ser executado onde o tratamento representar alto risco à garantia dos princípios gerais de proteção de dados pessoais previstos nesta Lei. Desta forma, mesmo que de maneira proativa, é recomendável que a FAB elabore tal relatório para as Solicitações de Autorização para Voo de Aeronaves Remotamente Pilotadas (SARPAS) para que, uma vez identificados os riscos à privacidade no Relatório de Risco dos Sistemas da Informação deste sistema, o COMAER possa discutir os controles mitigatórios a serem implementados de maneira a diminuir o nível destes riscos ao menor patamar possível.	
Resultado esperado	Elaborar o Relatório de Impacto à Proteção de Dados Pessoais.	
Referências	1) Art. 10, § 3º da Lei nº 13.709/2018.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

85 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a prestação dos Serviços de Tráfego Aéreo.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada registro que contenha dados pessoais tratados neste processo no âmbito dos sistemas utilizados para submissão do plano de voo, para o pagamento das tarifas de navegação ou para a apuração e aplicação das penalidades devidas. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 22.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

86 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a emissão de autorizações para utilização de Aeronaves Não Tripuladas.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada registro que contenha dados pessoais tratados neste processo no âmbito do sistema utilizado para solicitação de acesso ao Espaço Aéreo para o uso de Sistemas de Aeronaves Remotamente Pilotadas (RPAS/DRONES). Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 23.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

87 **Risco alto**	**É necessário que a FAB estabeleça sua Política de Privacidade específica para o serviço onde é possível Solicitar Autorização para Voo de Aeronaves Remotamente Pilotadas.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Convém que o DECEA elabore uma declaração quanto ao apoio e comprometimento para alcançar o *compliance* com a LGPD, assim como pretende garantir a segurança e a proteção dos dados pessoais tratados neste processo. O serviço fornecido através do Sistema de Solicitação de Acesso ao Espaço Aéreo por Aeronaves Não Tripulada (SARPAS) tem como público-alvo pessoas físicas e jurídicas de diferentes naturezas e que podem não ter nenhum outro tipo de vínculo com a FAB. Desta forma, através da elaboração de uma Política de Privacidade específica para este serviço o COMAER alcançará não somente o *compliance* com a Lei, como também demonstrará a seus titulares o seu comprometimento com a transparência, um dos pilares da LGPD. Esta atividade também será importante para diminuir os riscos identificados no sistema SARPAS presentes no Relatório de Risco dos Sistemas da Informação da FAB.	
Resultado esperado	Elaborar a Política de Privacidade aos usuários do sistema SARPAS.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 6.2.1.1). 3) ISO/IEC 29151:2017 (A2). 4) RTD nº 23.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

88 Risco alto	**Implementar um aviso de privacidade ao Serviço de Atendimento ao Cidadão do DECEA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário *web* de comunicação para o envio de dúvidas, sugestões, comentários, críticas, elogios e notificações de erros para que os titulares ao preencherem este formulário estejam cientes de como seus dados pessoais serão tratados e protegidos durante o atendimento a esta demanda. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade no formulário do Serviço de Atendimento ao Cidadão do DECEA.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.12.1 DECEA/ICEA

89 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a formação e capacitação realizada pelo ICEA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito dos sistemas utilizados para esta finalidade, como no Portal do ICEA e no SGEW, mas também nos registros armazenados fisicamente nas instalações do ICEA. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 40 e Art. 15 - I e II da Lei nº 13.709/2018. 2) RTD nº 24.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

90 Risco alto	**Implementar aviso de privacidade na Ficha de Indicação para os Cursos disponibilizados pelo ICEA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha de Indicação de Curso para que os titulares estejam cientes de como seus dados pessoais serão tratados e protegidos durante o atendimento a esta demanda. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade na Ficha de Indicação para o Curso.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 24.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

91 Risco alto	**Implementar aviso de privacidade na Ficha de Proposta de Estrangeiros para Participação nos cursos do ICEA.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha de Proposta de Estrangeiros para Participação nos cursos do ICEA para que os estrangeiros que tiverem interesse nos cursos ofertados pelo ICEA estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. A Ficha de Proposta está disponível no Portal do ICEA, em Catálogo Completo para Estrangeiros. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade na Ficha de Proposta de Estrangeiros para Participação nos cursos do ICEA.	
Referências	1) Art. 6, I e Art. 50, §2º, I, "a)" da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 24.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

92 Risco médio	**Considerar os conceitos de *Privacy by Design* em todo o ciclo de desenvolvimento do sistema SGEW.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Os conceitos de *Privacy by Desing* e *Privacy by Default* estão presentes em diversos pontos da Lei nº 13.709/2018 e auxiliam que consideravelmente no cumprimento das demais regulamentações de coleta, armazenamento, utilização e descarte das informações pessoais. Desta forma é importante que os princípios propostos nesta teoria sejam considerados em todo ciclo de vida do software em especial durante as etapas de design, codificação, testes, lançamento e manutenção.	
Resultado esperado	Implementar os princípios do *Privacy by Design* no ciclo de desenvolvimento do software.	
Referências	1) Art. 46, §2º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 5.4.1.2). 3) ISO/IEC 29151:2017 (Item 14.2.10). 4) RTD nº 24.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.13 EMAER

93 Risco médio	**Estabelecer o plano de trabalho com funções e responsabilidades do Encarregado de Dados do COMAER.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Uma vez indicado e com suas informações divulgadas é importante que o Encarregado esteja apto a exercer suas funções que, além de ser o elo de comunicação com a Autoridade Nacional e a sociedade também tem um papel fundamental na implementação do Programa de Governança em Privacidade do COMAER. Desta forma, é recomendável que seja estabelecido um plano de trabalho com as funções e as responsabilidades do Encarregado para que o mesmo tenha condições de bem desempenhar tal papel, com respaldo da Lei e da DCA 16-6/21.	
Resultado esperado	Assessorar o Encarregado do COMAER sobre suas funções e responsabilidades.	
Referências	1) Art. 41, § 2º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 6.3.1.1). 3) Art. 2º da IN SGD/ME Nº 117. 4) DCA 16-6.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

94 **Risco alto**	**Convém que a organização determine e documente um processo pelo qual possa demonstrar se, quando e como o consentimento para o tratamento de dados pessoais foi obtido, quando o enquadramento nessa base legal for pertinente.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	É recomendável que a organização estabeleça processo apto a demonstrar a forma e a data na qual o consentimento foi obtido dos titulares de dados pessoais para aqueles processos de negócio onde se faça necessária à coleta de consentimento para a realização do tratamento de dados pessoais, em função dessa hipótese de tratamento, quando a situação assim o exigir. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Implementar o fluxo de gestão do consentimento.	
Referências	1) Art. 8º - §2º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.2.3).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

95 **Risco alto**	**Convém que a organização forneça mecanismos para que os titulares de dados possam modificar ou cancelar os seus consentimentos.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Convém que a organização informe aos titulares dos dados sobre os seus direitos relativos ao cancelamento do consentimento a qualquer tempo, e forneça o mecanismo para fazê-lo. O mecanismo usado para cancelamento depende do sistema; convém que ele seja consistente com os mecanismos usados para a obtenção do consentimento, quando possível. Por exemplo, se o consentimento é coletado por e-mail ou por formulário *web*, convém que o mecanismo para cancelamento seja o mesmo, e não uma solução alternativa, como telefone ou fax. Convém que a organização registre qualquer solicitação para cancelar ou mudar o consentimento de uma forma similar ao registro do consentimento propriamente dito. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Implementar o fluxo de gestão do consentimento.	
Referências	1) Art. 8º, §2º e §5º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.3.4).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

96 **Risco alto**	**Convém que a organização estabeleça e implemente fluxos, políticas, procedimentos e/ou mecanismos para atender às suas obrigações para os titulares de dados acessarem, corrigirem e/ou excluírem os seus dados pessoais.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Convém que a organização implemente fluxos, políticas, procedimentos e/ou mecanismos para permitir aos titulares obter acesso para corrigir e excluir os seus dados pessoais, quando solicitado e sem atraso indevido. É importante que a organização defina um tempo de resposta e que a solicitação seja tratada de acordo com isto. Quaisquer correções ou exclusões deverão ser disseminadas por todos os sistemas e/ou para os usuários autorizados e também para aqueles para os quais os dados pessoais (coletados pela FAB) foram transferidos. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Implementar o fluxo de atendimento às solicitações.	
Referências	1) Art. 8º, §2º e §5º, Art. 19 da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.3.6). 3) ISO/IEC 29151:2017 (Item A.10.1).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

97 **Risco alto**	**É necessário que o COMAER estabeleça sua Política de Privacidade.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Convém que a organização produza uma declaração de comprometimento para o alcance da *compliance* com a LGPD, com termos contratuais acordados entre a organização e seus parceiros, subcontratados e seus terceiros aplicáveis (clientes, fornecedores etc.), para os quais convém que se especifiquem claramente as responsabilidades entre eles.	
Resultado esperado	Elaborar e publicar a Política de Privacidade do COMAER.	
Referências	1) Art. 6, I, Art. 23 e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 6.2.1.1). 3) ISO/IEC 29151:2017 (Item A2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

98 Risco médio	**Convém que uma política com medidas que apoiam a segurança da informação seja implementada para proteger as informações acessadas, processadas ou armazenadas em locais de trabalho remoto.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É importante que a FAB defina e publique, no cenário atual onde o trabalho remoto se tornou uma realidade para muitas pessoas e áreas, uma política que defina as condições e restrições para o uso do trabalho remoto considerando itens como os requisitos de segurança nas comunicações, levando em consideração a necessidade do acesso remoto aos sistemas internos da organização, a sensibilidade da informação que será acessada e trafegada na linha de comunicação e a sensibilidade do sistema interno. Trata-se de um documento muito importante para a manutenção da segurança da informação na FAB, uma vez que devem conter os aspectos técnicos do acesso que será realizado.	
Resultado esperado	Implementar políticas e procedimentos referentes ao trabalho remoto.	
Referências	1) ABNT NBR ISO/IEC 27002:2013 (Item 6.2.2).	
Gap associado	Ausência de Controles de Segurança em Redes, Proteção Física e do Ambiente.	

99 Risco médio	**Convém que todos os militares do COMAER recebam treinamento, educação e conscientização apropriados, bem como atualizações regulares das políticas e procedimentos organizacionais relevantes para as suas funções.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Convém que medidas sejam implementadas, incluindo a conscientização sobre notificação de incidentes, para assegurar que membros relevantes estejam cientes das possíveis consequências para a organização (por exemplo, consequências legais, perda de negócios e dano reputacional ou da marca), para os membros da organização (por exemplo, consequências disciplinares) e para o titular (por exemplo, consequências físicas, materiais e emocionais) da violação de privacidade ou de regras de segurança e procedimentos, especialmente aqueles relacionados ao manuseio de dados pessoais.	
Resultado esperado	Implementar um programa de conscientização.	
Referências	1) Art. 50, I, “a)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.2.2).	
Gap associado	Ausência de mecanismos de conscientização sobre a importância da Privacidade e Segurança da Informação.	

100 **Risco baixo**	**Convém que a organização assegure que os arquivos temporários criados como um resultado de tratamento de dados pessoais sejam descartados (por exemplo, apagados ou destruídos) seguindo procedimentos documentados dentro de um período especificado.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É importante que a organização assegure, através da apresentação de procedimento específico, que os usuários, ao tratar de dados pessoais, se preocupem com a exclusão dos arquivos temporários gerados durante seu processamento a fim de que planilhas ou documentos não fiquem armazenados nos computadores pessoais de cada um ao final do tratamento realizado. Além disso, é importante orientar também sobre o não armazenamento de informações oficiais do COMAER nos computadores locais dos militares, devendo sempre priorizar os sistemas e os ambientes em conformidade com as boas práticas de segurança da informação.	
Resultado esperado	Conscientizar o efetivo a eliminar arquivos temporários após sua utilização, especialmente aqueles que não mais atendam a finalidade para qual foram coletados, além de priorizar a utilização dos ambientes seguros.	
Referências	1) ABNT NBR ISO/IEC 27701 (Item 7.4.6). 2) ISO/IEC 29151:2017 (Item A.7.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

101 **Risco alto**	**Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas e ordenadas quando da identificação de violações de dados pessoais, bem como um plano para a gestão de crise.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Como os incidentes de violação de dados pessoais podem gerar grandes consequências se não forem devidamente controlados, é de extrema importância a criação de um processo maduro de gestão de crise que auxilie a FAB a suportar todos os cenários de uma crise, desde a sua identificação até a sua superação e levantamentos de lições aprendidas. Como parte do processo de gestão de incidentes de segurança da informação de modo global, convém que a organização estabeleça responsabilidades e procedimentos para a identificação e registro de violações de dados pessoais. Adicionalmente, convém que a organização estabeleça responsabilidades e procedimentos relativos à notificação para as partes envolvidas nas violações de dados (incluindo o tempo de tais notificações) e à divulgação para a ANPD.	
Resultado esperado	Estabelecer e implantar procedimentos de resposta a incidentes de segurança da informação e gestão de crise que representem violações de dados pessoais.	
Referências	1) Art. 50, I, “g)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 6.13.1.1 e 6.13.1.5).	
Gap associado	Ausência de procedimento de resposta a incidentes.	

102 **Risco médio**	**Convém que a organização avalie e implemente, onde apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de dados pessoais ou mudanças ao tratamento existente forem planejados.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	O tratamento de dados pessoais gera riscos para os titulares. Convém que estes riscos sejam analisados por meio de uma avaliação de impacto de privacidade (*Privacy Impact Analysis* - PIA). Os critérios, considerados para a decisão de avaliar ou não um processo, podem incluir a produção de efeitos legais nos titulares ou o tratamento em larga escala de categorias especiais de dados (por exemplo, informação relativa à saúde, origem étnica ou racial, opiniões políticas, crenças religiosas ou filosóficas, membros de sindicatos, dados de biometria ou dados genéticos).	
Resultado esperado	Realizar a avaliação sistemática de impactos e riscos à privacidade.	
Referências	1) Art. 50, I, “d)” da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.2.5).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

103 **Risco baixo**	**Convém que a organização defina e implemente, onde apropriado, uma avaliação de legítimo interesse quando houver a opção por justificar ou for aplicável a utilização da base legal do legítimo Interesse.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	O tratamento de dados pessoais deverá sempre ser baseado nas hipóteses legais apresentadas nos artigos 7º e 11 da Lei nº 13.709/2018. Caso a hipótese escolhida seja o legítimo interesse (Art. 7º, IX) a FAB deverá implementar uma Avaliação de Legítimo Interesse (*Legitimate Interests Assessment* - LIA) que deverá ser realizada antes do início do processamento de dados. Através da LIA será possível a avaliação de risco de se utilizar tal hipótese com base no contexto e nas circunstâncias específicas. Convém também que o COMAER registre e armazene tais Avaliações para demonstrar conformidade com suas obrigações legais. A Autoridade Nacional Inglesa detalha melhor e dá um exemplo deste tipo de documento auxiliar: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/legitimate-interests/how-do-we-apply-legitimate-interests-in-practice/	
Resultado esperado	Aplicar a Avaliação de Legítimo Interesse a novos processos que utilizarem como base esta hipótese legal.	
Referências	1) Art. 10 da Lei nº 13.709/2018.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

104 Risco alto	**Convém que a organização registre a transferência de dados pessoais para terceiros e assegure a cooperação com estas partes para apoiar futuras solicitações relativas às obrigações para os titulares de dados.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Registros podem incluir transferências de terceiros de dados pessoais que tenham sido modificados como um resultado das suas obrigações no gerenciamento dos controladores, ou na transferência para terceiros para implementar solicitações legítimas dos titulares, incluindo solicitações para exclusão dos dados (por exemplo, após o consentimento do cancelamento). Convém que a organização aplique o princípio de minimização dos dados para os registros de transferência, retendo apenas as informações estritamente necessárias e que estas transferências também sigam o Decreto 10.046/2019, quando tal compartilhamento de dados se der no âmbito da administração pública federal.	
Resultado esperado	Registrar todos os processos de transferências de dados pessoais.	
Referências	1) Art. 7º da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 7.5.3). 3) ISO/IEC 29151:2017 (Item A.13.2). 4) Decreto nº 10.046/2019, Capítulo III.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

105 Risco baixo	**Definir e implementar um processo de avaliação contínua do nível de conformidade do COMAER em relação às práticas de privacidade propostas pela LGPD.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Convém que o COMAER desenvolva e implemente um processo de avaliação contínua para monitoramento do nível de conformidade da organização no que diz respeito às práticas de privacidade propostas pela LGPD. Desta forma, a Organização terá uma visão mais assertiva sobre sua evolução acerca dos aspectos apresentados na legislação de privacidade e proteção de dados pessoais.	
Resultado esperado	Implementar processo de avaliação contínua de conformidade.	
Referências	1) ABNT NBR ISO/IEC 27701 (Item 6.15.2.3).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

106 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a indicação de militares para as Missões de Paz.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, como os registros armazenados nos servidores de arquivos do EMAER, dentre eles as certidões e cópias de formulários. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 49.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

107 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados no escopo das atividades exercidas pelas adidâncias militares no exterior.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados durante a execução das atividades das adidâncias, principalmente, os dados de seus funcionários que são armazenados em servidores de arquivos locais. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 50.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

108 Risco médio	É recomendável a elaboração de normativo acerca da gestão de dados pessoais nas adidâncias militares no exterior.	
	Controle: NORMATIVO	Prazo: 30/JUN/22
Descrição do controle	Como as adidâncias militares no exterior realizam diversas atividades em que se faz necessária à coleta e o tratamento de dados pessoais, não só de brasileiros, mas também de cidadãos de outras nacionalidades, é recomendável que seja elaborado documento que oriente as adidâncias quanto ao tratamento de dados considerando os princípios não só da LGPD, mas de frameworks internacionais de privacidade, uma vez que este tratamento pode ser alvo de outros regulamentos locais de privacidade.	
Resultado esperado	Elaborar normativo interno sobre a gestão de dados no âmbito das adidâncias militares no exterior.	
Referências	1) Art. 6º, X da Lei nº 13.709/2018. 2) RTD nº 50.	
Gap associado	Ausência de medidas de responsabilização.	

109 Risco alto	É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados coletados durante a execução do Programa Forças no Esporte (PROFESP).	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais sensíveis tratados durante a execução do programa, especialmente, os dados das crianças e adolescentes que participam deste programa. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 11, Art. 15 - I e II, da Lei nº 13.709/2018. 2) RTD nº 52.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

110 **Risco alto**	**É necessária a revisão do Termo de Adesão ao Serviço Voluntário no Programa Forças no Esporte.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Durante a execução das atividades do programa são utilizados voluntários que podem não ter nenhum tipo de vínculo com a FAB. Desta forma, é recomendável que o Termo por eles assinados seja revisado de modo a certificarem que estão cientes de que seus dados pessoais serão tratados somente durante a execução deste processo, bem como no reforço do papel do voluntário na manutenção da segurança e da privacidade dos dados coletados durante as atividades do programa. É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no Termo para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Revisar o Termo de Adesão ao Serviço Voluntário no PROFESP.	
Referências	1) Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 52.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

111 **Risco alto**	**É necessária a revisão da Ficha de Cadastro e Autorização para Prática Esportiva utilizada no Programa Forças no Esporte.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Para que as crianças tenham acesso aos serviços prestados no Programa Forças no Esporte é necessário o preenchimento de ficha de cadastro com a autorização dos pais e responsáveis, bem como o fornecimento de diversas informações pessoais dos menores que integrarão o programa. Desta forma é necessário que a ficha de cadastro seja revisada para deixar claro que os dados pessoais serão tratados somente durante a execução deste processo, bem como com a inserção de item destacado para a coleta de consentimento dos pais e responsáveis quanto ao fornecimento dos dados dos menores ao COMAER para a execução deste programa. É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e apenas para essa finalidade. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Revisar a Ficha de Cadastro e Autorização para a participação no PROFESP.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 52.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

112 Risco alto	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais dos menores que participam do Programa Forças no Esporte (PROFESP).**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Os pais que procuram as Forças Armadas para candidatarem seus filhos no PROFESP, serão submetidos a critérios de seleção definidos pelas FFAA. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados pessoais coletados dos titulares responsáveis, bem como dos dependentes menores (dados pessoais sensíveis). Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais coletados para o PROFESP e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações sensíveis.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 11, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2).	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

113 Risco alto	**Implementar aviso de privacidade no Sistema de Gestão Estratégica da Aeronáutica (GPAer).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (privacy notice) no Sistema de Gestão Estratégica da Aeronáutica (GPAer) para que os usuários estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade no Sistema de Gestão Estratégica da Aeronáutica (GPAer).	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2).	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.14 GABAER

114 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante as avaliações para concessão de medalha, condecoração ou membro honorário.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento que contenha dados pessoais tratados neste processo de formação de dossiê avaliativo para as concessões. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 44.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

115 **Risco alto**	**Implementar aviso de privacidade na Ficha de Proposta para concessão de medalha, condecoração ou membro honorário.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha de Proposta para concessão de medalha, condecoração ou membro honorário, para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade na Ficha de Proposta para concessão de medalha, condecoração ou membro honorário.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 44.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

116 Risco alto	É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais do público externo submetido a avaliação para concessão de medalha, condecoração ou membro honorário.	
	Controle: TECNOLÓGICO	Prazo: 14/DEZ/23
Descrição do controle	Para os indicados serem agraciados com a concessão de medalha, condecoração ou membro honorário, serão submetidos a critérios de escolha definidos pelo GABAER. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados pessoais coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular (externos ao COMAER) um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais de titulares externos ao COMAER e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 44.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

5.15 SEFA

117 Risco alto	É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados através da entrega das declarações de bens e valores.	
	Controle: PROCESSUAL	Prazo: 15/DEZ/22
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento recebido que contenha dados pessoais tratados durante o fornecimento, por orientação legal, da declaração de bens e valores, como por exemplo as declarações de impostos de renda entregues pelos agentes da administração que gerenciam recursos financeiros. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 53.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

118 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante os processos de compra ou de contratação.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados em todos os processos de aquisição ou contratação no âmbito do COMAER. Considerando que a SEFA é a dona dessa regra de negócio, entende-se que será a responsável por promover e padronizar essa adequação em toda a FAB. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 46.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

119 **Risco alto**	**É necessário que todas as aquisições, contratações ou parcerias que forem realizadas pelo COMAER considerem os aspectos da Lei nº 13.709/2018.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Os agentes de tratamento, segundo a LGPD, têm entre suas responsabilidades a de adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais. A LGPD também afirma que a responsabilidade sobre violação de dados que ocorrer mediante ao não atendimento à legislação recairá sobre os agentes de tratamento. Diante disso é fundamental que estas medidas sejam tomadas desde o momento que se estabelece uma relação contratual ou de parceria com um operador para que sejam estabelecidas as responsabilidades e atribuições de cada uma das partes durante o tratamento de dados que ocorrerá mediante esta vigência contratual.	
Resultado esperado	Elaborar contratos com cláusulas de proteção de dados pessoais e expedir modelos de cláusulas para utilização geral do COMAER.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 38 e 46.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

120 Risco alto	**Revisar o contrato com a empresa que presta serviço de crédito consignado com a Força Aérea Brasileira.**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	Considerado que o COMAER utiliza os serviços da empresa Zetra, que é especializada em proporcionar mais facilidade ao Militar/Pensionista e uma maior competitividade entre as Entidades Consignatárias, é importante que este instrumento legal seja revisto para que o mesmo possua todas as cláusulas referentes à atividade de operador realizada pela empresa segundo à LGPD, uma vez que durante a natureza desta atividade a empresa têm acesso a inúmeros dados pessoais e confidenciais dos militares da FAB.	
Resultado esperado	Revisar e adequar o contrato à LGPD.	
Referências	1) Art. 39 e Art. 50, § 1º da Lei nº 13.709/2018. 2) RTD nº 35.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

121 Risco alto	**É recomendável que seja definido um procedimento padrão para o tratamento dos dados pessoais do público externo que possui relação contratual ou de parceria com o COMAER.**	
	Controle: TECNOLÓGICO	**Prazo: 14/DEZ/23**
Descrição do controle	Para que um cidadão se torne parceiro ou prestador de serviços junto ao COMAER, será submetido a critérios de escolha definidos por instrumento contratual. Com isso, ao tornarem público tais critérios, deverão ser apresentadas também a finalidade e a temporalidade para a realização do tratamento dos dados pessoais coletados dos titulares. Assim, essas informações pessoais deverão ser inseridas em um sistema capaz de entregar ao titular (externos ao COMAER) um mecanismo de gerenciamento próprio dos seus dados, conforme determina a Lei, tudo para o controlador não correr o risco de realizar o tratamento após alcançada sua finalidade. A DTI deverá apoiar neste processo, conforme descrito na ação 32.	
Resultado esperado	Padronizar os procedimentos de guarda dos dados pessoais de titulares externos ao COMAER e implantar, até o final do prazo, um sistema centralizado capaz de gerenciar tais informações.	
Referências	1) Art. 6º, V, Art. 8º - §2º, Art. 15 - I e II, da Lei nº 13.709/2018. 2) ABNT NBR ISO/IEC 27701 (Item 11.1.2). 3) RTD nº 38 e 46.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

122 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a administração dos Próprios Nacionais Residenciais (PNR).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito dos documentos apresentados fisicamente às Organizações Militares, mas também nos registros armazenados nos servidores de arquivos e bancos de dados das Prefeituras de Aeronáutica. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 36.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

123 Risco médio	**É recomendável definir um cadastro padronizado e unificado dos Próprios Nacionais Residenciais (PNR), bem como implementar um aviso de privacidade nesse cadastro.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Como cada prefeitura apresenta sua própria maneira de receber, guardar e armazenar os dados coletados durante a administração dos PNR e desta forma não há garantias quanto à segurança, temporalidade e rastreabilidade de acesso aos dados pessoais é recomendado que se crie procedimento padrão, bem como um sistema, para o tratamento de tais informações, de modo a ter condições de garantir a segurança dos dados coletados e garantir também o atendimento aos demais requisitos da Lei nº 13.709/2018. É necessário que seja acrescentado aviso de privacidade (*privacy notice*) na Ficha cadastral para ocupação dos PNR, para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade na Ficha cadastral para ocupação de PNR.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 36.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

124 Risco alto	**Revisar o normativo que regulamenta a administração dos Próprios Nacionais Residenciais (PNR).**	
	Controle: NORMATIVO	**Prazo: 30/JUN/22**
Descrição do controle	ICA 12-20/2019 tem como objetivo regulamentar a administração de Próprios Nacionais Residenciais (PNR). Desta forma se faz necessário a revisão de tal documento para que os anexos que solicitam informações pessoais dos titulares estejam ajustados aos ditames da Lei nº 13.709/2018. Especial atenção deverá ser dada aos anexos "I", "L", "P", "Q", "R", "S", e "W".	
Resultado esperado	Adequar a ICA 12-20/2019 à LGPD.	
Referências	1) Art. 6º, I, II, III, V, VI e X da Lei nº 13.709/2018. 2) RTD nº 36.	
Gap associado	Ausência de medidas para assegurar o *Compliance* com a Privacidade.	

125 Risco alto	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados pelos Hotéis de Trânsito (HT).**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito dos formulários de reserva enviados por e-mail aos hotéis, mas também nas fichas de hotelaria geradas e armazenados localmente nos HT. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 37.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

126 **Risco médio**	**É recomendável definir um formulário padronizado para ser utilizado nos Hotéis de Trânsito (HT), bem como implementar um aviso de privacidade nesse formulário.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Como cada HT possui sua própria dinâmica para receber, guardar e armazenar os dados coletados durante suas atividades de gestão hoteleira e da forma como é realizado atualmente não há garantias quanto à segurança, temporalidade e rastreabilidade de acesso aos dados pessoais, é recomendado que se crie procedimento padrão, bem como um sistema, para o tratamento de tais informações de modo a ter condições de garantir a segurança dos dados coletados e garantir também o atendimento aos demais requisitos da Lei nº 13.709/2018. É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário de hospedagem para ocupação dos HT, para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade no formulário de hospedagem para ocupação de Hotel de Trânsito.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 37.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

5.15.1 SEFA/DIRAD

127 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais tratados durante a execução do pagamento de pessoal.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito dos sistemas utilizados para esta finalidade, mas também nos registros armazenados nos servidores de arquivos e bancos de dados da SDPP. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 35.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

5.15.2 SEFA/DIRAD/BREVET

128 **Risco alto**	**É necessária a aplicação da política de temporalidade e destinação final aos dados pessoais dos inativos e dos pensionistas geridos pela BREVET.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	Segundo a LGPD, os dados pessoais só podem permanecer na base de dados até a ocorrência de um dos requisitos elencados em seu art. 15. Desta forma, é necessário que sejam aplicadas as diretrizes sobre o prazo de guarda aplicado a cada documento/registro que contenha dados pessoais tratados neste processo, não só no âmbito documentos físicos recebidos durante os atendimentos realizados, mas também no escopo dos sistemas utilizados para tramitação dos mesmos. Também é recomendável que, ao alcançar o tempo de guarda previsto na fase intermediária, os documentos/registros utilizados para esta finalidade sigam as orientações para aplicação da destinação final para eles definidos através das diretrizes de Gestão Documental no âmbito do COMAER.	
Resultado esperado	Aplicar os critérios de temporalidade aos documentos/registros físicos e digitais utilizados durante a execução do processo.	
Referências	1) Art. 15 - I e II, Art. 40 da Lei nº 13.709/2018. 2) RTD nº 47.	
Gap associado	Ausência de Tabela de Temporalidade e Destinação Final definidas.	

129 **Risco alto**	**Implementar aviso de privacidade no formulário de cadastro ao canal de comunicação Reserva Interativa.**	
	Controle: PROCESSUAL	**Prazo: 15/DEZ/22**
Descrição do controle	É necessário que seja acrescentado aviso de privacidade (*privacy notice*) no formulário de cadastro no Reserva Interativa, para que os titulares estejam cientes de que seus dados pessoais serão tratados somente durante a execução deste processo e que este tratamento ocorrerá de acordo com as boas práticas de proteção e privacidade de dados. Disponível em: <https://www.fab.mil.br/reservainterativa> Ao final deste documento (Anexo A) é apresentado um modelo de aviso de privacidade para orientar acerca da definição deste item.	
Resultado esperado	Implementar o Aviso de Privacidade na Ficha de Proposta para concessão de medalha, condecoração ou membro honorário.	
Referências	1) Art. 6, I e Art. 50, §2º, I, “a)” da Lei nº 13.709/2018. 2) ISO/IEC 29151:2017 (Item A.4.2). 3) RTD nº 47.	
Gap associado	Ausência de medidas para garantir a Abertura, Transparência e Notificação.	

6 DISPOSIÇÕES FINAIS

Este Plano deve ser atualizado por iniciativa do Estado-Maior da Aeronáutica, em coordenação com os ODSA, sempre que julgado necessário, pois a implementação destes controles não garantirá a conformidade definitiva, por ser tratar de um processo cíclico e a realização de seu gerenciamento contínuo é fundamental para garantir a manutenção da adequação à LGPD.

REFERÊNCIAS

BRASIL. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO 31000:2018** - Gestão de Riscos – Diretrizes. 2018.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013:** Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos. 2013.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27002:2013:** Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação. 2013.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 27701:2019** Sistema de Gerenciamento de Informações de Privacidade (PIMS). 2019.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 29134:2020** Tecnologia da informação - Técnicas de segurança - Avaliação de impacto de privacidade - Diretrizes. 2020.

_____. Associação Brasileira de Normas Técnicas. **ABNT NBR ISO/IEC 29151:2020** Tecnologia da informação - Técnicas de segurança - Código de prática para proteção de dados pessoais. 2020.

_____. Comando da Aeronáutica. Centro de Documentação da Aeronáutica. “Confecção, Controle e Numeração de Publicações Oficiais do Comando da Aeronáutica”: **NSCA 5-1**. Rio de Janeiro, RJ, 2011.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Gestão de Riscos no COMAER”: **DCA 16-2.** Brasília, DF, 2018.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Gestão por Processos no COMAER”: **DCA 16-5.** Brasília, DF, 2019.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Glossário da Aeronáutica”: **MCA 10-4**. Brasília, DF, 2001.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Governança da Proteção de Dados Pessoais do COMAER”: **DCA 16-6.** Brasília, DF, 2021.

_____. Comando da Aeronáutica. Estado-Maior da Aeronáutica. “Governança no COMAER”: **DCA 16-1.** Brasília, DF, 2019.

_____. Lei nº 8.159, de 8 de janeiro de 1991. Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

_____. Lei nº 12.527, de 18 de novembro de 2011. Regula o acesso às informações (Lei de Acesso à Informação - LAI).

_____. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).

_____. Ministério da Defesa. “Código de classificação e tabela de temporalidade e destinação de documentos de arquivo relativos às atividades-fim do Ministério da Defesa”. Brasília, DF, 2013.

_____. Ministério da Justiça. “Código de classificação e tabela de temporalidade e destinação de documentos relativos às atividades-meio do Poder Executivo Federal”. Rio de Janeiro, RJ, 2020.

_____. Resolução CD/ANPD nº 1, de 28 de outubro de 2021 Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador no âmbito da Autoridade Nacional de Proteção de Dados.

Gartner Group. Beyond GDPR: **5 Best Practices for LGPD Compliance**. Disponível em: <https://www.gartner.com/en/documents/3903476/beyond-gdpr-5-best-practices-for-lgpd-compliance>

ANEXO A

PRIVACY NOTICE

Este anexo é destinado para auxiliar a melhor compreensão e elaboração do Comando da Aeronáutica quanto ao *Privacy Notice* ou aviso de privacidade.

Privacy Notice ou é um pequeno texto de caráter público que explica como é realizado o tratamento de dados pessoais e devem conter informações quanto ao que será feito com estes dados, de modo a indicar quais dados pessoais serão utilizados, para qual finalidade e por quanto tempo.

O aviso de privacidade deve ser acrescentado aos documentos ou formulários em que o Titular de dados fornecer suas informações pessoais, podendo variar conforme cada especificidade.

Em razão disso, serão apresentados dois exemplos de *Privacy Notice* que nortearão o melhor entendimento para diversas possíveis aplicações:

I. “Suas informações pessoais serão tratadas pelo Comando da Aeronáutica com a finalidade de executar políticas públicas voltadas a defesa nacional, com isso, apesar do enquadramento no Art. 4º, inciso III, letra “b” isentar a Organização da aplicação da Lei, os dados serão tratados com adequação as finalidades informadas ao titular no momento da coleta, seguindo o princípio da necessidade, que limita o tratamento ao mínimo necessário para a realização das respectivas finalidades, bem como dentro da temporalidade prevista em Lei.”

II. “Quando nosso site é acessado exclusivamente para obter informações, ou seja, quando você não se registra ou nos fornece informações de qualquer outra forma, apenas coletamos os dados pessoais fornecidos pelo seu navegador ao nosso servidor. Quando você realizar o *login* (acessar à área reservada) no nosso site, coletamos alguns dados necessários para fins técnicos para podermos demonstrar nosso site a você e para garantir a estabilidade e a segurança de acesso adequadas (IP, Hora do Acesso, Navegador, Sistema Operacional). Esses dados são retidos por razões de segurança (por exemplo, para investigação de uso indevido ou prevenção de fraude) por no máximo sete dias e excluídos após o vencimento. Os dados que devem ser retidos por um período mais longo, como evidência, só serão excluídos após o incidente relevante ser finalmente esclarecido.”

ANEXO B

DADOS ESTATÍSTICOS DAS AÇÕES