MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

POLÍTICA

DCA 14-8

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA

2022

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
ESTADO-MAIOR DA AERONÁUTICA

POLÍTICA

DCA 14-8

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMANDO DA AERONÁUTICA

2022

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
GABINETE DO COMANDANTE DA AERONÁUTICA

PORTARIA GABAER N° 273/GC3, DE 18 DE ABRIL DE 2022.

Aprova a Diretriz que estabelece a Política de Segurança da Informação do Comando da Aeronáutica.

O **COMANDANTE DA AERONÁUTICA**, no uso das atribuições que lhe confere o inciso I e XIV do Art. 23 da Estrutura Regimental do Comando da Aeronáutica, aprovada pelo Decreto nº 6.834, de 30 de abril de 2009, e considerando o que consta no Processo nº 67050.003688/2022-89, procedente do Estado-Maior da Aeronáutica, resolve:

Art. 1º Aprovar a reedição da DCA 14-8 "Política de Segurança da Informação do Comando da Aeronáutica", que com esta baixa.

Art. 2º Esta Portaria entra em vigor em 2 de maio de 2022.

Ten Brig Ar CARLOS DE ALMEIDA BAPTISTA JUNIOR
Comandante da Aeronáutica

SUMÁRIO

PREFÁCIO

Na era da informação em que vivemos não há dúvida de que o conteúdo informacional de uma organização - considerado um de seus principais patrimônios - está sob constante risco. Dessa maneira, a Segurança da Informação tornou-se um ponto crucial para a sobrevivência das instituições públicas e privadas e, em particular, para o cumprimento da missão institucional do Comando da Aeronáutica (COMAER).

Em um contexto mundial, as informações contidas em sistemas computacionais são consideradas ativos críticos - tanto para a concretização dos negócios de uma organização como para a tomada de decisão em questões governamentais, sociais, educativas e outras – necessitando, dessa maneira, que a segurança seja gerida de forma absoluta. Tal realidade não é diferente no âmbito do COMAER, onde cada vez mais se projetam sistemas corporativos sob o enfoque gerencial ou transacional, com vistas a auxiliar o processo de tomada de decisão, pois o valor da informação vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. E em um mundo interconectado, a própria informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações, são ativos que têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

As facilidades no acesso a ferramentas de ataque disponíveis na Internet aumentam significativamente a exposição dos ativos informacionais a novas ameaças. Diante disso, faz-se necessário cuidado contra ações ofensivas aos sistemas do COMAER. Essas ações sempre visam comprometer pessoas, processos, infraestruturas de comunicação e, consequentemente, os requisitos de confidencialidade, de integridade e de disponibilidade da informação e suas tecnologias associadas. Ademais, as ações ofensivas adquirem uma maior expectativa de êxito quando da ausência de uma gestão de riscos integrada a um modelo de gestão definido para o gerenciamento de uma Segurança da Informação que somente é alcançada com a implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos e estrutura organizacional. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados para assegurar que os objetivos e a Segurança da Informação sejam atendidos.

Diante do exposto, um sistema de informação focado no uso da TI, para operar de forma adequada e prover a Segurança da Informação, disponível em formato digital, necessita de ambientes controlados e protegidos contra desastres naturais (incêndio, terremoto e enchente), falhas estruturais (interrupção do fornecimento de energia elétrica, sobrecargas elétricas e outros), sabotagem, fraudes, acessos não autorizados (hackers, espionagem industrial, venda de informações confidenciais) e outros tipos de ameaças que gerem riscos não aceitáveis e que, consequentemente, necessitam ser tratados e monitorados constantemente.

Por fim, a Segurança da Informação representa a preparação do ambiente para a aplicação operacional da defesa cibernética, de modo que a elaboração e a adoção de uma Política de Segurança da Informação evidenciam o comprometimento da alta administração com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão desse processo de segurança na organização.

1 DISPOSIÇÕES PRELIMINARES

1.1 FINALIDADE

Esta Diretriz tem por têm por finalidade orientar o planejamento e execução das ações relacionadas com a Segurança da Informação no âmbito do COMAER, observando o disposto na Estratégia de Governo Digital, Decreto nº 10.332, de 28 de abril de 2020, na Política Nacional de Segurança da Informação, Decreto nº 9.637, de 26 de dezembro de 2018, na Estratégia Nacional de Segurança Cibernética, Decreto nº 10.222, de 5 de fevereiro de 2020, na Estratégia Nacional de Segurança de Infraestruturas Críticas, Decreto nº 10.569, de 9 de dezembro de 2020, na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020 e na Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021.

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 Glossário de Segurança da Informação (Portaria GSI/PR nº 93, de 26 de setembro de 2019).

1.3 ÂMBITO

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

2 DIRETRIZES E PREMISSAS

2.1 PRINCÍPIOS

2.1.1 A informação é um recurso vital para o adequado funcionamento das Organizações do COMAER, devendo ser tratada como patrimônio a ser protegido e preservado de modo proativo, com o objetivo de assegurar o cumprimento da missão institucional.

2.1.2 A Segurança da Informação no COMAER compreende um conjunto de objetivos, diretrizes, normativas gerenciais e técnicas, e demais controles destinados a garantir a confidencialidade, a disponibilidade, a integridade, a irretratabilidade e a autenticidade da informação em todo o seu ciclo de vida, disponibilizada ou em trânsito em ambiente digital ou físico.

2.1.3 A Segurança da Informação além de fundamentar as ações de adequação à privacidade de dados, abrangerá também, a Segurança Cibernética, a Defesa Cibernética, a segurança física e a proteção de dados e ativos de informação, conforme destacado no Art. 2º do Decreto nº 9.637, de 26 de dezembro de 2018 que institui a Política Nacional de Segurança da Informação e dispõe sobre a Governança da Segurança da Informação.

2.1.4 O sucesso das ações nos assuntos de Segurança da Informação está diretamente associado à capacitação científico-tecnológica do capital humano envolvido, à conscientização do público interno, à qualidade das soluções adotadas e à proteção das informações contra ameaças internas e externas.

2.1.5 A exploração pelo COMAER de tecnologias consagradas pelo uso, tais como a Internet, a Intranet, o correio eletrônico, a infraestrutura de chaves públicas, dentre outras, deve ser disciplinada em documentos normativos gerenciais e técnicos, respeitando as diretrizes de segurança traçadas por esta Política.

2.1.6 Todo ativo de informação produzido ou processado no Sistema de Tecnologia da Informação da Aeronáutica (STI) e demais ativos considerados críticos no Sistema devem ser claramente identificados, inventariados e submetidos a procedimentos de segurança e a análise de riscos continuada, baseados em uma metodologia formalizada que identifique as ameaças a que estão expostos e os níveis de probabilidade e de impacto diante de um incidente de segurança, a fim de mensurar qualitativamente os riscos e selecionar os controles necessários à garantia da confidencialidade, da integridade e da disponibilidade da informação.

2.2 INFRAESTRUTURAS CRÍTICAS

2.2.1 De acordo com o Decreto nº 10.569, de 9 de dezembro de 2020, que aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas, essas infraestruturas necessitam de medidas de segurança capazes de garantir sua integridade e seu funcionamento, o que significa dizer que a segurança física e operacional precisa ser conhecida e acompanhada, a fim de assegurar a prestação desses serviços essenciais, sendo que a segurança efetiva se inicia com a compreensão clara de todos os tipos e níveis de risco que uma organização enfrenta.

2.2.2 O Tribunal de Contas da União (TCU) realizou auditoria e expediu o Acórdão nº 1.889/2020–TCU-Plenário, de 22/07/2020, que teve como objetivo identificar os sistemas informacionais críticos na Administração Pública Federal e elaborar diagnóstico da capacidade de fiscalização das unidades técnicas com foco nesses sistemas.

2.2.3 Por ocasião dessa auditoria, os sistemas informacionais críticos e suas respectivas criticidades foram oficializados pelo COMAER junto ao TCU, até que ocorra revisão técnica emergencial dessa priorização, conforme se segue:

a) SISDABRA/SISCEAB (Criticidade ALTA);

b) CTIR.FAB (Criticidade ALTA);

c) SIGADAER (Criticidade MÉDIA);

d) SIGPES (Criticidade BAIXA); e

e) SILOMS (Criticidade BAIXA).

2.2.4 Com isso, as diretrizes e, especialmente, os processos estabelecidos por esta Política deverão ser priorizados e aplicados aos sistemas considerados críticos, pois a Instituição sofrerá novas auditorias e fiscalizações mais detalhadas sobre a adoção dos procedimentos previstos neste documento.

2.2.5 Para a futura reclassificação da criticidade dos sistemas do COMAER poderá ser adotada a aplicação dos 22 parâmetros selecionados e descritos no referido Acórdão, como base norteadora.

2.3 DEFESA CIBERNÉTICA

2.3.1 A Defesa Cibernética é, de acordo com a Estratégia Militar de Defesa Cibernética, o conjunto de ações ofensivas, defensivas e exploratórias, realizadas no Espaço Cibernético, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa, com as finalidades de proteger os sistemas de informação de interesse da Defesa Nacional, obter dados para a produção de conhecimento de Inteligência e comprometer os sistemas de informação do oponente.

2.3.2 Assim, quando a temática "cibernética" é abordada, normalmente ocorre o entendimento de que a denominação está restrita ao âmbito interno das Força Armadas, voltada para a "Guerra Cibernética", em seu nível tático.

2.3.3 Contudo, é importante destacar que a Política de Segurança da Informação do COMAER representa a tradução das ações demandadas pelo nível político, que, de forma mais ampla, servirão de preparação para as ações de Defesa e de Guerra Cibernética a serem desenvolvidas pela Força.

2.3.4 Assim, o futuro Centro de Defesa Cibernética da Aeronáutica (CDCAER), na condição de Órgão Central do futuro Sistema de Defesa Cibernética (SISDCAER), deverá desempenhar atribuições de Segurança da Informação, Comunicações e Segurança Cibernética, conforme normativos definidos pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR), em conjunto com o Órgão Central do Sistema de Tecnologia da Informação (STI) e do Serviço de Telecomunicações do Comando da Aeronáutica (STCA), para o alcance dos seus objetivos nos campos da Defesa e da Guerra Cibernética, em prol do Poder Aeroespacial.

2.4 PRIVACIDADE DE DADOS PESSOAIS

2.4.1 A privacidade de dados pessoais está diretamente associada à Segurança da Informação e aos recursos computacionais devido ao grande envolvimento com as etapas do ciclo de vida da informação, que tem um ciclo natural, indo desde a sua criação e origem, armazenagem, processamento, uso e transmissão, até a sua eventual destruição e obsolescência.

2.4.2 Desenvolvimento de sistemas novos e mudanças nos sistemas existentes são boas oportunidades para as organizações atualizarem e melhorarem os controles de segurança, levando em conta os incidentes reais e os riscos de Segurança da Informação, projetados e atuais.

2.4.3 A DCA 16-6/2021, que trata da Governança da Proteção de Dados Pessoais do COMAER, traz em seu item 3.7 boas práticas em Segurança da Informação voltadas para a Privacidade de Dados com foco em conceitos como privacidade desde a concepção e por padrão (*PRIVACY BY DESIGN AND BY DEFAULT*).

2.5 TRANSFORMAÇÃO DIGITAL

2.5.1 Em atenção ao Decreto nº 10.332, de 28 de abril 2020, que trata Estratégia de Governo Digital para o período de 2020 a 2022, o COMAER atualizou sua carta de serviços ao usuário disponibilizando ao Cidadão o conteúdo acessível no seguinte canal: <https://www.gov.br/pt-br/orgaos/comando-da-aeronautica>.

2.5.2 Esses serviços requerem atenção de Segurança e de Privacidade devido à grande interação com os órgãos externos, por utilizarem recursos como o *login* único do Governo Federal, o Módulo de Avaliação do usuário, o PAGTESOURO, a base de dados para prova de vida *online* e a identificação militar disponibilizada em formato digital.

2.5.3 Com isso, as organizações responsáveis pela disponibilidade dos referidos serviços necessitam observar e aplicar as diretrizes e os processos previstos nesta Política, para resguardar o COMAER, inclusive quando forem abertos novos serviços transformados digitalmente, unificados canais digitais ou promovida a interoperabilidade entre os sistemas.

2.6 TRATAMENTO DA INFORMAÇÃO

2.6.1 O Centro de Inteligência da Aeronáutica (CIAER) publicou diversas orientações que estão em vigor e que devem ser colocadas em prática por todos os integrantes do COMAER, conforme descritas abaixo:

a) FCA 200-2/2008 “Mentalidade de Segurança”;

b) FCA 200-3/2009 “Prevenção à Engenharia Social”; e

c) FCA 200-6/2013 “Guia prático de execução de medidas do decreto de tratamento de informações classificadas no COMAER”.

2.7 SEGURANÇA FÍSICA E DO AMBIENTE

2.7.1 A implementação dos controles de segurança e proteção contra ameaças físicas e ambientais trará mais do que uma proteção para a informação. Estes controles contribuem para a proteção dos ativos que representam valor para a organização, exigindo atenção e dedicação da administração com os cuidados com a segurança de equipamentos que contém esses ativos de informação, instalados em locais definidos como áreas seguras.

2.7.2 A segurança de equipamentos deverá contemplar os processos de instalação e proteção, as manutenções (preditivas, preventivas e corretivas), a segurança dos cabeamentos e, também, a política de segurança de equipamentos utilizados em trabalho remoto, ou seja, fora das dependências da organização, além de dispositivos móveis.

2.7.3 A áreas seguras requerem, no mínimo, controles de entrada física, segurança contra incêndio, controle de climatização das salas cofre e sistemas de energia em redundância.

2.8 CONTROLES DE ACESSO

2.8.1 Todas as organizações do COMAER devem considerar os controles de acesso lógico e físico utilizando, no mínimo, das orientações da norma ABNT NBR ISO/IEC 27002:2013 - Código de prática para controles de Segurança da Informação.

2.8.2 O controle de acesso, na Segurança da Informação, é composto dos processos de autenticação, autorização e auditoria. Nesse contexto, o controle de acesso pode ser entendido como a habilidade de permitir ou negar a utilização de um objeto (uma entidade passiva, como um sistema ou arquivo) por um sujeito (uma entidade ativa, como um indivíduo ou um processo). A autenticação confirma a identidade do usuário (pessoa ou outro sistema) que acessa o sistema, a autorização determina o que um usuário autenticado pode executar e a auditoria diz o que o usuário fez.

2.8.3 As políticas de controle de acesso deverão ser orientadas pelos princípios da necessidade de conhecer e da necessidade de uso, logo, para acessar a informação ou os recursos de processamento de informação (equipamentos de TI, aplicações, procedimentos, salas etc.) o usuário somente deverá ter acesso às informações necessárias para o desempenho específico das suas tarefas ou funções.

2.8.4 As regras para a elaboração dessas políticas deverão ser definidas pelo STI.

2.9 GESTÃO DE USO DE RECURSOS OPERACIONAIS E DE COMUNICAÇÃO

2.9.1 Deverá ser atualizada a norma, que trata da Segurança da Informação e Defesa Cibernética em nível operacional/tático. Ela deve conter inúmeras políticas de uso de recursos computacionais e de comunicação e representa um modelo de canal técnico/normativo para incorporar outras políticas como a utilização de e-mail e correio eletrônico, o acesso à internet, o gerenciamento de senhas e identificação, o uso de VPN, as mídias sociais, a computação em nuvem, os controles criptográficos, a política de cookies, a política de privacidade de dados, entre outras.

2.9.2 Sobre as comunicações é fortemente recomendado que a responsabilidade operacional pelas redes seja separada da operação dos recursos computacionais administrativos. Ou seja, a segregação entre as redes operacional e administrativa representará um incremento na segurança dos serviços da rede.

2.9.3 Sobre tal segregação, deve haver um monitoramento de ambas as redes com uso de *firewalls* de borda para a proteção de perímetro das redes, possibilitando o controle de tráfego de informações com as redes externas por um Centro de Operações de Rede (NOC) e a gestão da segurança, por um Centro de Operações de Segurança (SOC), de modo que toda essa infraestrutura de proteção de perímetro seja gerenciada por um NOC/SOC, a exemplo da que se encontra em operação no NuCGTEC (PAME-RJ).

2.9.4 A limitação e o controle nos pontos de entrada para a rede interna e corporativa apontam para o elevado nível segurança almejado na utilização da rede de dados do COMAER.

2.9.5 Desse modo, quaisquer saídas para a rede externa (como a Internet), sejam elas originadas das redes operacionais ou administrativas, devem passar por dispositivos (*firewalls*) que permitam o controle de perímetro e possam ser gerenciadas por um NOC e também possibilitem a gestão da segurança pelo SOC. Assim, essas saídas devem ser previamente autorizadas pelo NOC/SOC.

2.9.6 Não obstante, quaisquer infraestruturas computacionais deverão ter, a critério dos responsáveis, seus respectivos *firewalls* de aplicação, contendo políticas de segurança específicas, enquanto os *firewalls* de borda implementarão as políticas gerais de proteção das redes do COMAER.

3 PROCESSOS

O Art. 12 da IN nº 1, 27/05/20 (GSI/PR), propõe uma composição mínima para a elaboração de uma Política de Segurança da Informação (POSIN), de modo que os principais processos previstos na IN nº 3, 28/05/21 (GSI/PR), compõem essas exigências mínimas e, por esse motivo, serão abordados nesta POSIN-FAB, que tem como objetivo a busca pelo alinhamento com a evolução da tecnologia e de seus riscos, identificando os fatores internos e externos que podem impactar no alcance dos objetivos do COMAER, além da necessidade de ser mantida e implementada continuamente.

3.1 MAPEAMENTO DE ATIVOS DE INFORMAÇÃO

3.1.1 O processo de mapeamento de ativos de informação tem o objetivo de estruturar e manter um registro de ativos de informação, destinados a subsidiar os processos de gestão de risco, de gestão de continuidade e de gestão de mudanças, especialmente nos aspectos relativos à Segurança da Informação (Art.4º - IN nº 3).

3.1.2 O registro de ativo de informação resultantes do processo de mapeamento de ativos de informação deverá conter (Art. 6º - IN nº 3):

a) os responsáveis - proprietários e custodiantes de cada ativo de informação;

b) informações básicas sobre os requisitos de Segurança da Informação de cada ativo de informação;

c) os contêineres de cada ativo de informação; e

d) as interfaces de cada ativo de informação e as interdependências entre eles.

3.1.3 Para o COMAER, caberá ao Órgão Central do STI (DTI) a coordenação do processo de mapeamento de ativos de informação, bem como designar os agentes responsáveis pela gestão desses ativos de informação.

3.1.4 E caberá aos agentes responsáveis pela gestão dos ativos de informação cumprir as determinações do Art. 9º da IN nº 3.

3.2 GESTÃO DE RISCO E VULNERABILIDADES

3.2.1 A vulnerabilidade é o ponto onde qualquer sistema é suscetível a um ataque, ou seja, é uma condição encontrada em determinados recursos, processos e configurações, causada muitas vezes pela ausência ou ineficiência das medidas de proteção para salvaguardar os bens da organização. (MOREIRA, 2001)

3.2.2 Desse modo, a gestão do Risco visa a identificação, a análise e a avaliação destas vulnerabilidades, com o objetivo de se mitigar tais fragilidades, buscando o aprimoramento dos mecanismos de tratamento de riscos de Segurança da Informação.

3.2.3 Em atenção aos Art. 13, 14 e 15, da IN nº3, o plano de gestão de risco da Segurança da Informação deverá ser produto de um trabalho conjunto, sendo elaborado e conduzido pelo Órgão Central do STI, passando a ser conduzido pelo futuro Órgão Central do Sistema de Defesa Cibernética da Aeronáutica (SISDCAER), após a publicação do seu ato de criação.

3.3 GESTÃO DE CONTINUIDADE E *BACKUP*

3.3.1 Em função do Acórdão nº 1.109/2021-TCU-Plenário, os gestores deverão ser orientados a "regulamentar a obrigatoriedade de que as entidades e órgãos públicos aprovem formalmente e mantenham atualizadas políticas gerais e planos específicos de *backup* (para suas bases de dados e sistemas críticos, por exemplo), contemplando requisitos mínimos para endereçar os cinco subcontroles do controle 10 (*Data Recovery Capabilities*) do framework preconizado pelo *Center for Internet Security* (CIS), em especial quanto à definição do escopo dos dados a serem copiados, suas respectivas periodicidades, tipos, quantidades de cópias, locais de armazenamento, tempos de retenção e outros requisitos de segurança."

3.3.2 A implementação do processo de gestão de continuidade de negócios em Segurança da Informação tem o objetivo de minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do órgão nessa área, além de recuperar perdas de ativos de informação em nível aceitável, por intermédio de ações de resposta a incidentes e recuperação de desastres (Art.18º - IN nº3).

3.3.3 Para isso, deverão ser adotadas as demais orientações previstas na IN nº3, com destaque para a elaboração do Plano de Continuidade, sob a coordenação e responsabilidade do Órgão Central do STI, que revisará anualmente do referido plano, priorizando sempre os sistemas críticos.

3.3.4 O Órgão Central do STI poderá designar agentes responsável pela referida gestão, nas unidades em que forem identificadas atividades críticas, desde que apliquem as atribuições e responsabilidades previstas nos Art. 26 e 27 da IN nº 3.

3.4 GESTÃO DE MUDANÇA

3.4.1 A implementação do processo de gestão de mudanças nos aspectos de Segurança da Informação tem por objetivo preparar e adaptar as Organizações para as mudanças decorrentes da evolução de processos e de Tecnologias da Informação, visando à obtenção de mudanças eficazes e eficientes e à mitigação de eventuais resistências. (Art. 28 - IN nº 3).

3.4.2 O processo de gestão de mudanças nos aspectos de Segurança da Informação deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos, bem como no relatório de tratamento desses riscos de Segurança da Informação.

3.4.3 O processo mencionado em 3.4.1, além de promover o controle das mudanças planejadas, deve considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

3.4.4 Conforme o Art. 29 - IN nº 3, a mudança pode ser classificada como emergencial, rotineira ou proativa.

3.4.5 Para o COMAER, a condução no processo de Gestão de Mudança será de responsabilidade do Órgão Central do STI, que deverá adotar as demais providências previstas na IN nº 3.

3.5 AUDITORIA E AVALIAÇÃO DE CONFORMIDADE

3.5.1 A avaliação de conformidade nos aspectos de Segurança da Informação consiste em proporcionar adequado grau de confiança a um determinado processo, mediante o atendimento de requisitos definidos em políticas, procedimentos, normas ou em regulamentos técnicos aplicáveis. (§3º, Art. 37 - IN nº 3).

3.5.2 Caberá ao Órgão Central do SISDCAER, com apoio do EMAER, a condução da avaliação de conformidade nos aspectos de Segurança da Informação no COMAER, conforme descritos na IN nº3, bem como na DCA 11-130 (Implantação do NuCDCAER), item 1.5.3, letra "a".

3.5.3 E caberá ao Órgão Central do STI a implantação e a operação do servidor centralizado para armazenamento de logs do ambiente de infraestrutura de TIC, como instrumento para as auditorias.

3.6 GESTÃO DE INCIDENTES

3.6.1 Por orientação do GSI-PR as Equipes de Tratamento e Resposta a Incidentes Cibernéticos deverão ser compostas, preferencialmente, por servidores públicos civis ocupantes de cargo efetivo ou militares de carreira, com capacitação técnica compatível com as atividades dessa equipe (§3º, Art. 22 - IN nº 1).

3.6.2 A atuação da Equipe será regida por normativos, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta de Incidentes Cibernéticos do Governo, sem prejuízo das demais metodologias e padrões conhecidos, ou por normas internas, a exemplo da ICA 7-42, que trata do Gerenciamento de Incidentes de Segurança em Redes de Computadores do COMAER, desde que atualizadas com periodicidade de até 4 (quatro) anos.

3.6.3 A estrutura constituída do CTIR.FAB deverá estar sob a responsabilidade do Órgão Central do SISDCAER, conforme DCA 11-130 (Implantação do NuCDCAER), item 1.5.2, letras "a" e "b".

4 COMITÊ DE SEGURANÇA DA INFORMAÇÃO

4.1 COMPOSIÇÃO

4.1.1 Em cumprimento ao Art. 15 do Decreto nº 9.637, de 26 de dezembro de 2018, que Institui a Política Nacional de Segurança da Informação (PNSI), o COMAER define que o comitê de Segurança da Informação interno será composto pelo:

a) gestor da Segurança da Informação (Oficial General): responsável pelo Órgão Central do SISDCAER e pela coordenação desta Política;

b) representante do EMAER (Oficial General): Encarregado de tratamento de dados pessoais;

c) representante de cada unidade finalística (Oficial General); e

d) titular da unidade de tecnologia da informação e comunicação (Oficial General): Responsável pelo Órgão Central do STI.

4.1.2 Em proveito da similaridade com o previsto no decreto nº 10.332, de 28 de abril de 2020, que Institui a Estratégia de Governo Digital para o período de 2020 a 2022 e que também exige a instituição de um comitê equivalente, o Comitê de Governança Digital, com a participação dos indicados no item 4.1.1, ficará responsável por reunir e pautar os assuntos relativos à Segurança da Informação desta Política, bem como à Privacidade de Dados previstos na DCA 16-6/21, sem o prejuízo das demandas relativas à Governança de TI do COMAER.

4.1.3 Por analogia à PNSI, em seu Art. 10, o Comitê se reunirá, em caráter ordinário, semestralmente e, em caráter extraordinário, por convocação de seu responsável.

4.2 COMPETÊNCIAS

4.2.1 Observar que a importância do Comitê tem por finalidade articular o desenvolvimento de um processo de segurança preventiva de recursos humanos, de equipamentos, de instalações, de serviços, de sistemas, de informação e de outros recursos que, de alguma forma, assegurem a resiliência e o funcionamento dos serviços e das atividades do COMAER que dependem das informações e suas tecnologias associadas.

4.2.2 Manter em contínuo aperfeiçoamento a identificação e a classificação das infraestruturas informacionais críticas.

4.2.3 Assessorar na implementação das ações de Segurança da Informação.

4.2.4 Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e indicar pessoas capazes de cumprir com as responsabilidades.

4.2.5 Propor alterações na Política de Segurança da Informação e propor normas internas relativas à Segurança da Informação.

5 ATRIBUIÇÕES E RESPONSABILIDADES

De acordo com a ABNT NBR ISO/IEC 27002:2013 muitas organizações atribuem a um gestor de Segurança da Informação a responsabilidade global pelo desenvolvimento e implementação dessa segurança, além de apoiar na identificação de controles, entretanto, a responsabilidade por pesquisar e implementar tais controles frequentemente permanecerá com gestores individuais, pois uma política comum é a nomeação de um proprietário para cada ativo de informação que, então, se torna responsável por sua proteção no dia-a-dia.

5.1 CECOMSAER

5.1.1 Estabelecer e executar um programa contínuo de conscientização sobre a segurança da informação, a proteção e a privacidade dos dados pessoais para todo o efetivo do COMAER.

5.1.2 Promover a ampla divulgação da DCA 14-8 que trata da "Política de Segurança da Informação do COMAER."

5.2 CIAER

5.2.1 Atualizar os normativos descritos em 2.6.1, com periodicidade de até 4 (quatro) anos, e publicar outras normas que considerar aderentes a esta Política, caso necessário.

5.3 COMGAP

5.3.1 ÓRGÃO CENTRAL DO SISDCAER

5.3.1.1 Promover, com apoio da alta administração e do CECOMSAER, a divulgação da Política, das normas internas de Segurança da Informação e de suas atualizações, de forma ampla e acessível, a todos os servidores, aos usuários e aos prestadores de serviço, a fim de que esses tomem conhecimento de tais instrumentos.

5.3.1.2 Promover ações de capacitação e profissionalização dos recursos humanos em temas relacionados à Segurança da Informação.

5.3.1.3 Planejar a execução de programas, de projetos e de processos relativos à Segurança da Informação, objetivando o aumento da resiliência dos ativos de tecnologia da informação e comunicação e dos serviços definidos como infraestrutura crítica ou estratégicos pelo Comitê.

5.3.1.4 Implantar mecanismo de comunicação imediata sobre a existência de vulnerabilidades ou incidentes de segurança que impactem ou possam impactar os serviços prestados pelo COMAER.

5.3.1.5 Estabelecer diretrizes e implementar os controles para o processo de gestão de riscos de Segurança da Informação.

5.3.1.6 Consolidar e analisar os resultados dos trabalhos de auditoria sobre a gestão de Segurança da Informação.

5.3.1.7 Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da Segurança da Informação.

5.3.1.8 Manter contato direto com o Departamento de Segurança da Informação do GSI/PR em assuntos relativos à Segurança da Informação.

5.3.1.9 Definir políticas, procedimentos, normas ou regulamentos técnicos para a condução da avaliação de conformidade nos aspectos de Segurança da Informação do COMAER.

5.3.1.10 Informar ao EMAER imediatamente as situações as quais ficam sujeitas as consequências e as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre os militares e os servidores do COMAER relativas ao assunto.

5.3.1.11 Realizar avaliação técnica para redefinir a priorização e a criticidade dos sistemas informacionais críticos do COMAER, com o apoio dos ODGSA, conforme premissas do item 2.2 e em até 180 (cento e oitenta) dias após a entrada em vigor desta Diretriz.

5.3.1.12 As atribuições definidas para o Órgão Central do SISDCAER nesta Política ficarão a cargo do Órgão Central do STI, até que a Portaria de criação do SISDCAER seja publicada e a subordinação do CDCAER seja definida.

5.3.2 ÓRGÃO CENTRAL DO STI

5.3.2.1 Promover a simplificação administrativa, a modernização da gestão pública e a integração dos serviços públicos, especialmente aqueles prestados por meio eletrônico, com vistas à Segurança da Informação.

5.3.2.2 Apresentar ao EMAER as evidências sobre a implementação dos mecanismos de descoberta, inventário e controles de ativos (hardware e software) e de sistemas desenvolvidos ou mantidos pelo COMAER, em até 30 (trinta) dias após a entrada em vigor desta Diretriz e em concordância com o processo descrito no item 3.1.3.

5.3.2.3 Apresentar ao EMAER as evidências sobre a atualização da política de gestão de risco e de vulnerabilidades e das práticas implementadas, em até 30 (trinta) dias após a entrada em vigor desta Diretriz e em concordância com o processo descrito no item 3.2.3.

5.3.2.4 Apresentar ao EMAER as evidências sobre a atualização da política de gestão de controle de acesso lógico e das práticas implementadas, em até 30 (trinta) dias após a entrada em vigor desta Diretriz e em concordância com a premissa descrita no item 2.8.

5.3.2.5 Atualizar a NSCA 7-13/2013, que trata da Segurança da Informação e Defesa Cibernética, em até 30 (trinta) dias após a entrada em vigor desta Diretriz.

5.3.2.6 Apresentar ao EMAER as evidências sobre a implementação das práticas previstas na política de backup e no processo de ampliação dos respectivos controles, decorrentes das aquisições de hardware e software planejados para o corrente ano, até o dia 30 de novembro de 2022 e em concordância com o processo descrito no item 3.3.

5.3.2.7 Apresentar ao EMAER as evidências sobre a implantação e a operação do servidor centralizado para armazenamento de logs do ambiente de infraestrutura de TIC, como instrumento para as auditorias internas, até o dia 30 de novembro de 2022.

5.3.2.8 Implantar o processo de gestão de mudança no COMAER até o dia 30 de novembro de 2022, em concordância com o processo descrito no item 3.4.

5.4 COMGEP

5.4.1 Estabelecer meios de captação de recursos humanos especializados nas áreas de interesse da Segurança da Informação do COMAER, em coordenação com o EMAER, a DTI e o CIAER.

5.5 COMPREP

5.5.1 Realizar estudos sobre as premissas apresentadas nos itens 2.8, em coordenação com Órgão Central do STI, relativas à publicação ou à atualização da política de gestão de controle de acessos físico, em função da Segurança da Informação, na vertente segurança física das instalações, e apresentar os resultados ao Comitê, em até 180 (cento e oitenta) dias após a entrada em vigor desta Diretriz.

5.6 DECEA

5.6.1 Realizar estudos sobre as premissas apresentadas nos itens 2.9.2 até 2.9.6 e apresentar os resultados ao Comitê, em até 180 (cento e oitenta) dias após a entrada em vigor desta Diretriz.

5.6.2 Atualizar as legislações que tratam de Segurança da Informação no âmbito do DECEA, em coordenação com Órgão Central do STI, em até 180 (cento e oitenta) dias após a entrada em vigor desta Diretriz.

5.7 EMAER

5.7.1 Monitorar o desempenho e avaliar a concepção, a implementação e os resultados da sua política e das normas internas de Segurança da Informação.

5.7.2 Destinar recursos orçamentários para ações de Segurança da Informação.

5.7.3 Apoiar o Órgão Central do SISDCAER na definição de políticas, procedimentos, normas ou regulamentos técnicos para a condução da avaliação de conformidade nos aspectos de Segurança da Informação do COMAER.

5.7.4 Publicar anualmente em portaria a atualização dos componentes do Comitê de Segurança da Informação do COMAER.

6 DISPOSIÇÕES FINAIS

6.1 O Estado-Maior da Aeronáutica deve receber, analisar e aplicar as penalidades para os casos de violação da Política de Segurança da Informação ou de quebra de segurança, de acordo com as normas já existentes no ordenamento jurídico vigente sobre os militares e os servidores do COMAER relativas ao assunto.

6.2 Esta Diretriz deve ser atualizada por iniciativa do EMAER, em coordenação com os ODSA, sempre que julgado necessário, desde que realizada em até 4 (quatro) anos, conforme orientações do §1º, item VII do Art. 12 da Instrução Normativa nº 1, de 27 de maio de 2020 (GSI/PR).

REFERÊNCIAS

BRASIL. 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.

_____. 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. "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.

_____. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação.

_____. Decreto nº 9.832, de 12 de junho de 2019. Dispõe sobre o Comitê Gestor da Segurança da Informação.

_____. Decreto nº 10.222, de 5 de fevereiro de 2020. Aprova a Estratégia Nacional de Segurança Cibernética.

_____. Decreto nº 10.332, de 28 de abril de 2020. Institui a Estratégia de Governo Digital para o período de 2020 a 2022.

_____. Decreto nº 10.569, de 9 de dezembro de 2020. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas.

_____. Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020. Dispõe sobre a Estrutura de Gestão da Segurança da Informação.

_____. Instrução Normativa GSI/PR nº 3, de 28 de maio de 2021. Dispõe sobre os processos relacionados à gestão de Segurança da Informação.

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

_____. Portaria GSI/PR nº 93, de 26 de setembro de 2019. Aprova o Glossário de Segurança da Informação.

_____. Tribunal de Contas da União. **Acórdão nº 1.109/2021**. Plenário. Relator: Ministro Vital do Rêgo. Sessão de 12/5/2021. "Procedimentos de Backup"

_____. Tribunal de Contas da União. **Acórdão nº 1.889/2020**. Plenário. Relator: Ministro Aroldo Cedraz. Sessão de 22/7/2020. "Sistemas Informacionais Críticos"

MOREIRA, Nilton Stringasci. Segurança Mínima. Rio de Janeiro: Axcel Books, 2001.