MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

PORTARIA DTI Nº 154/GOVS, DE 28 DE FEVEREIRO DE 2025.
Protocolo COMAER nº 67131.000414/2025-81

Aprova a Norma de Sistema que dispõe sobre a Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica.

O **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA**, no uso de suas atribuições lhe confere o art. 5º da Portaria nº 634/GC3, de 11 de dezembro de 2023, e art. 6º do Regulamento da Diretoria de Tecnologia da Informação da Aeronáutica, aprovado pela Portaria nº 905/GC3, de 4 de fevereiro de 2025, resolve:

Art. 1º Aprovar a Norma de Sistema (NSCA 7-13), na forma dos anexos I, II, III, IV, V, VI, VII, VIII, IX, X, XI, XII, XIII, XIV, XV, XVI, XVII, XVIII, XIX, XX, XXI, XXII, XXIII, XXIV, XXV, XXVI, XXVII e XXVIII para a Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica.

Art. 2º Revoga-se a Portaria COMGAP n° 42/ADLG, de 2 de maio de 2022, publicada no Boletim do Comando da Aeronáutica n°81, de 3 de maio de 2022.

Art. 3º Esta Portaria entra em vigor no primeiro dia útil da primeira semana subsequente a de sua publicação.

Brig Eng SÉRGIO RICARDO DE ASSIS

Diretor de Tecnologia da Informação da Aeronáutica

MINISTÉRIO DA DEFESA

COMANDO DA AERONÁUTICA

DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA

TECNOLOGIA DA INFORMAÇÃO

NSCA 7-13

SEGURANÇA DA INFORMAÇÃO E DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA

2025

ANEXO I

SEGURANÇA DA INFORMAÇÃO E DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA (NSCA 7–13)

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Finalidade

Art. 1º Orientar as Organizações do Comando da Aeronáutica (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 contribuir com a Proteção do Espaço Cibernético sob responsabilidade do Comando da Aeronáutica.

Seção II
Conceituações

Art. 2º Para efeito de entendimento desta Instrução, aplicam-se os termos e expressões com os significados constantes no Glossário das Forças Armadas (MD-35-G-01/2015), do Glossário de Segurança da informação (Portaria GSI/PR nº 93, de 18 de outubro de 2021), da Doutrina Militar de Defesa Cibernética (MD31-M-07/2023) e as seguintes conceituações:

I - acesso remoto à Intraer – acesso à Intraer originado fora de rede local de OM do COMAER;

II - acesso à Internet – estação de trabalho com acesso, via canalização de dados, à rede local de computadores de uma OM do COMAER, possuindo acesso aos sistemas e serviços disponibilizados na Intraer;

III - administrador de rede – é o militar ou civil designado pelo Comandante, Chefe, ou Diretor para administrar a rede local de computadores de uma Organização Militar (OM);

IV - apagamento seguro – processo por meio do qual os dados eliminados ficam definitivamente irrecuperáveis;

V - ataque cibernético (Atq Ciber) – compreende as ações no Espaço Cibernético para modificar, degradar, corromper, negar, interromper ou destruir os SCTIC², ativos de informação, infraestruturas ou meios de emprego militar de interesse das forças amigas;

VI - proteção cibernética (Ptç Ciber) – abrange as ações no Espaço Cibernético, preventivas e reativas, para mitigar, neutralizar ou impedir ataques e explorações cibernéticas contra os Sistemas de Comunicações e Tecnologia da Informação para Comando e Controle (SCTIC²), ativos de informação, infraestruturas ou meios de emprego militar de interesse das forças amigas. São ações de apoio à Proteção Cibernética todas as ações que diminuem a liberdade de ação das forças inimigas no espaço cibernético.

VII - BMP – serve como um número único que ajuda a identificar e rastrear cada item, junto com outras informações, como o identificador do ativo;

VIII - **Center for Internet Secutiry** (CIS) – é uma organização sem fins lucrativos, voltada para a comunidade de segurança. É responsável pelo **CIS Controls**, práticas recomendadas e mundialmente reconhecidas para proteger aplicações e dados nos ambientes de tecnologia;

IX - **Security Information and Event Management (SIEM)** – é uma ferramenta essencial para organizações que buscam proteger seus sistemas e dados contra ameaças cibernéticas, oferecendo uma abordagem proativa e integrada à segurança;

X - CMTAER – Comandante da Aeronáutica;

XI - conta de usuário – identificação individual de usuário, constituída por um código de usuário acompanhado de uma senha, a qual define os direitos de acesso do usuário aos Recursos Computacionais do COMAER;

XII - controle – conjunto de políticas, processos, procedimentos, estrutura organizacional e funções de **software** e/ou **hardware** que precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, quando necessário, para assegurar que os objetivos do negócio e a segurança da informação da organização sejam atendidos;

XIII - controle de acesso – conjunto de procedimentos de segurança que balizam os direitos de acesso e restrições para papéis específicos dos usuários acessarem os Recursos Computacionais, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados;

XIV - CTIR.FAB – sigla designativa para o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos da Força Aérea Brasileira, subordinado ao Órgão Central do Sistema de Tecnologia da Informação (STI) do COMAER e mantido pelo Centro de Defesa Cibernética da Aeronáutica (CDCAER);

XV - defesa cibernética (Def Ciber) – ações 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 ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação do oponente;

XVI - Elos de coordenação do STI – são setores da estrutura regimental dos Órgãos de Direção-Geral, Setorial e de Assistência Direta e Imediata ao Comandante da Aeronáutica (ODGSA) responsáveis por coordenar os assuntos de TI seus e das OM a ele subordinadas, junto ao Órgão Central do STI;

XVII - Elos especializados do STI – são OM do COMAER, definidas em ato específico do Órgão Central, que executam atividades ou serviços especializados de TI de interesse do COMAER.

XVIII - Elos de serviços do STI são estruturas, seções ou frações das OM do COMAER responsáveis pela prestação de serviços de TI para uma ou mais OM do COMAER, tais como a manutenção e segurança cibernética de Infraestrutura e de Serviços de TI locais, e apoio ao usuário;

XIX - Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) - grupo de agentes públicos com a responsabilidade de prestar serviços relacionados à segurança cibernética para o órgão ou a entidade da administração pública federal, em observância à política de segurança da informação e aos processos de gestão de riscos de segurança da informação do órgão ou da entidade. Anteriormente era chamada de Equipe de Tratamento de Incidentes de Rede;

XX - estações de trabalho – designação genérica dos microcomputadores conectados ou não à rede de dados, que são utilizados pelos usuários;

XXI - fatores de autenticação – fatores de autenticação são os diferentes tipos de informações ou mecanismos utilizados para verificar a identidade de um usuário durante um processo de autenticação. Eles fornecem uma camada adicional de segurança para garantir que apenas indivíduos autorizados tenham acesso a sistemas, dispositivos ou serviços. Os fatores de autenticação podem incluir algo que o usuário sabe (como senhas ou PINs), algo que o usuário possui (como celulares ou **tokens**) e algo que o usuário é (em geral traços biométricos, como impressão digital, reconhecimento facial ou voz). Ao combinar múltiplos fatores de autenticação (autenticação multifator - MFA), os sistemas podem fortalecer significativamente a segurança contra acessos não autorizados;

XXII - **firewall** externo – sistema de segurança de rede que controla o tráfego entre serviços da DMZ e clientes ou serviços da Internet;

XXIII - **firewall** interno – sistema de segurança de rede que controla o tráfego entre dispositivos e serviços da rede interna da OM com a Intraer ou com a DMZ;

XXIV - Lei Geral de Proteção de Dados Pessoais (LGPD) – Lei n° 13.709/2018, fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais;

XXV - **log** – registros de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação a serem mantidos e analisados criticamente, a intervalos regulares;

XXVI - não repúdio – habilidade de provar a ocorrência de um evento ou ação e suas entidades originárias;

XXVII - Órgão Operador – organização do COMAER responsável pela sustentação de um produto de TI após a sua implantação;

XXVIII - **patches** – atualizações de programas e sistemas operacionais disponibilizados pelos fabricantes, com a finalidade de corrigir erros (bugs) constatados durante o tempo de vida do **software** ou sistemas operacionais;

XXIX - **port-scan** – o ato de sistematicamente fazer varreduras de portas (local onde informações entram e saem) de Recursos Computacionais;

XXX - processo – conjunto de ações estruturadas, sistemáticas, medidas e formalizadas, visando a um certo resultado;

XXXI - Programa de Privacidade e Segurança da Informação (PPSI) - caracteriza-se como um conjunto de projetos e processos de adequação nas áreas de privacidade e segurança da informação e tem como valores: a maturidade, a resiliência, a efetividade, a colaboração e a inteligência;

XXXII - **Recovery Point Objective** (RPO) – define o máximo de dados que pode ser perdido em caso de uma falha ou incidente. Ele é medido em relação ao tempo decorrido desde o último **backup** realizado;

XXXIII - **Recovery Time Objective** (RTO) – define o tempo máximo aceitável para restaurar o serviço ou o sistema após uma falha ou incidente. Em outras palavras, é o prazo que a organização tem para retomar a operação normal;

XXXIV - recursos computacionais – são os equipamentos, as instalações, as redes de

computadores, os programas de computador e os bancos de dados administrados, mantidos ou operados pelo COMAER, que para efeito desta Norma, correspondem ao conjunto formado pelos ativos físicos, de informação e de **software**;

XXXV - recursos computacionais corporativos – recursos computacionais disponibilizados e utilizados no âmbito do COMAER cuja gerência é efetuada por um ODGSA;

XXXVI - recursos computacionais locais – recursos computacionais existentes, utilizados e administrados no âmbito de cada OM, cuja gerência é efetuada pelo Setor de TI dessa Organização;

XXXVII - redes sem fio – soluções técnicas de rede, cujo objetivo é estabelecer conectividade entre estações em uma rede local ou entre segmentos de redes locais, sem a utilização dos tradicionais cabos de pares trançados ou ópticos. O padrão adotado na implementação de redes sem fio é o recomendado na norma IEEE 802.11 (**Institute of Electrical and Eletronics Engineers**) e suas variantes;

XXXVIII - segurança cibernética – ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis;

XXXIX - senha – conjunto de caracteres, de conhecimento único do usuário, utilizado no processo de verificação de sua identidade, assegurando que ele é realmente quem diz ser e que possui o direito de acessar o recurso em questão;

XL - servidor – recurso computacional que desempenha alguma função de prestação de serviço de rede, tais como armazenamento de dados, impressão, acesso para usuários e outros;

XLI - sistema – conjunto de elementos integrantes e interdependentes, vinculados por meio de normalização específica, com a finalidade de dinamizar e aprimorar a comunicação e trâmites processuais entre os integrantes, conforme regras de negócios previamente definidas pelo Órgão Central do Sistema;

XLII - Sistema Militar de Defesa Cibernética (SMDC) – o SMDC é um conjunto de instalações, equipamentos, doutrina, procedimentos, tecnologias, serviços e pessoal essenciais para realizar ações voltadas para assegurar o uso efetivo do espaço cibernético pela Defesa Nacional, bem como impedir ou dificultar ações hostis contra seus interesses;

XLIII - **secure shell** (SSH) – protocolo que utiliza criptografia para acesso a um computador remoto, permitindo a execução de comandos, transferências de arquivos e outros;

XLIV - **smart card** – é um cartão que funciona como mídia armazenadora. Em seus chips são armazenadas as chaves privadas dos usuários. O acesso às informações neles contidas é feito por meio de senha pessoal, determinada pelo titular;

XLV - **spam** – termo usado para se referir aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;

XLVI - usuários de recursos de tecnologia da informação – para fins desta Política, consideram-se usuários de recursos de tecnologia da informação servidores ocupantes de cargo efetivo ou cargo em comissão, ocupantes de emprego público em exercício, assim como funcionários de empresas prestadoras de serviços, estagiários e demais usuários temporários em atividade no COMAER;

XLVII - videoconferência – solução técnica baseada em recursos de rede de dados que permite

o contato audiovisual entre pessoas ou grupos de pessoas que estão em lugares diferentes, através do uso de câmeras de videoconferência e de **software** específicos, baseados nos padrões preconizados nas normas do ITU (**International Telecommunication Union**);

XLVIII - varredura passiva – refere-se a uma técnica de monitoramento de rede que observa e analisa o tráfego de dados sem interferir ativamente no ambiente ou gerar tráfego adicional;

XLIX - (RBAC) – **Role-Based Access Control** – controle de acesso baseado em função;

L - VoIP – o termo **VoIP**, ou **Voice Over IP** ou Voz Sobre IP refere-se a soluções tecnológicas que permitem a digitalização de voz e a sua transmissão por redes de dados que utilizam o protocolo IP (**Internet Protocol**). Estas soluções são utilizadas, principalmente, para apoiar atividades de telefonia e videoconferência; e

LI - **Web Content Accessibility Guidelines** (WCAG) – conjunto de recomendações criado pelo **World Wide Web Consortium** (W3C), para tornar o conteúdo da web acessível a pessoas com diferentes tipos de deficiência, como visual, auditiva, motora ou cognitiva.

Seção III
Âmbito

Art. 3º Esta norma aplica-se a todas às OM do COMAER.

Seção IV
Objetivos

Art. 4º Elencar os princípios básicos a fim de garantir os níveis adequados de segurança da informação de ativos físicos, dos ativos de **software** e dos ativos de informação de interesse do COMAER.

Art. 5º Conscientizar os usuários de Tecnologia da Informação (TI) do COMAER e os colaboradores terceirizados sobre a importância de conhecer e aplicar as normas e os procedimentos de segurança da informação preconizados nas legislações inerentes ao assunto, tanto as publicadas na esfera do COMAER, quanto as publicadas em outras esferas governamentais.

Art. 6º Estabelecer as condições para operacionalização dos procedimentos de classificação, processamento, envio, armazenamento e descarte das informações sensíveis que integram os sistemas de TI.

Art. 7º Orientar quanto ao emprego adequado de certificados digitais, em conformidade com a Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), a fim de garantir a autenticidade e o não repúdio das transações que envolvem os ativos de informação de interesse do COMAER.

Art. 8º Definir os requisitos de segurança da informação nas atividades de contratação, de operação e de manutenção de sistemas aplicativos de TI em conformidade com as normas de segurança da informação estabelecidas no COMAER.

Art. 9º Conscientizar o público interno do Comando da Aeronáutica sobre as vulnerabilidades e riscos aos quais estão submetidos os recursos computacionais da Organização ou pessoais, seja para defesa

da infraestrutura crítica da informação, seja para possível resposta a ações ofensivas perpetradas por elementos adversos.

Art. 10. Assegurar o alinhamento das normas com os **CIS Controls®** V8 e o Guia Complementar de Privacidade e o Programa de Proteção e Segurança da Informação (PPSI) do Governo Federal, garantindo a conformidade com os padrões nacionais e internacionais de segurança da informação.

Art. 11. Consolidar a implementação das seguintes Políticas anexas à esta NSCA e estabelecer a obrigatoriedade do preenchimento do Termo de Ciência e Compromisso com as Políticas de Segurança da Informação (Anexo XIX):

I - Política de Uso de Recursos Computacionais (Anexo II);

II - Política de Administração de Recursos Computacionais (Anexo III);

III - Política de Manipulação de Informações Classificadas (Anexo IV);

IV - Política de Antivírus e Códigos Maliciosos (Anexo V);

V - Política de Firewall e Recursos Computacionais Localizados em Zonas Desmilitarizadas (Anexo VI);

VI - Política de Segurança Física (Anexo VII);

VII - Política de Segurança dos Serviços de Rede (Anexo VIII).

VIII - Política de Segurança em Servidores (Anexo IX);

IX - Política de Acesso Remoto (Anexo X);

X - Política de Segurança Lógica (Anexo XI);

XI - Política de Inspeção (Anexo XII);

XII - Política de Backup e Restauração de Dados Digitais (Anexo XIII);

XIII - Política de Gestão de Ativos (Anexo XIV);

XIV - Política de Gestão de Dados (Anexo XV);

XV - Política de Controle de Acesso (Anexo XVI);

XVI - Política de Gestão de Registros (logs) de Auditoria – PGRA (Anexo XVII);

XVII - Política de Defesa Contra Malware (Anexo XVIII);

XVIII - Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação (Anexo XX);

XIX - Política de Gerenciamento de Vulnerabilidades (Anexo XXI);

XX - Política de Gestão de Provedor de Serviços (Anexo XXIII);

XXI - Política de Proteção de Dados Pessoais (Anexo XXIV); e

XXII - Política de Acessibilidade Digital (Anexo XXV);

CAPÍTULO II
INVENTÁRIO E CONTROLE DE ATIVOS INSTITUCIONAIS

Seção I
Do inventário de ativos institucionais

Art. 12. O STI deve estabelecer e manter um inventário preciso, detalhado e atualizado de todos os ativos corporativos com potencial para armazenar ou processar dados, com revisão semestral, incluindo:

I - dispositivos de usuário final;

II - dispositivos de rede;

III - dispositivos não computacionais;

IV - dispositivos de IoT; e

V - servidores.

Art. 13. O inventário dos ativos institucionais deve registrar, pelo menos:

I - endereços de rede (se estático);

II - endereços de **hardware**;

III - nomes das máquinas;

IV - proprietários dos ativos de dados;

V - departamento para cada ativo; e

VI - se o ativo foi aprovado para se conectar à rede.

Art. 14. O inventário deve incluir todos os ativos conectados à infraestrutura, sejam físicos, virtuais, remotos ou em nuvem, incluindo aqueles conectados regularmente, mesmo que não estejam sob controle direto da OM. Cada ativo deve ter um responsável primário formalmente designado, conforme sua posição ou cargo.

Art. 15. Somente ativos que atendam aos critérios de segurança poderão se conectar à rede, incluindo:

I - sistema operacional dentro de seu ciclo de vida;

II - sistema operacional atualizado e com todos os **patches** de segurança aplicados; e

III - antivírus corporativo instalado e atualizado.

Parágrafo único. Princípios de privacidade devem ser incorporados ao inventário, considerando aspectos tecnológicos e processuais para proteger dados pessoais.

Art. 16. Ferramentas do tipo MDM (**Mobile Device Management**) devem oferecer suporte a esse processo em dispositivos móveis de usuário final, quando apropriado.

Seção II
Do endereçamento de ativos não autorizados

Art. 17. Os procedimentos para lidar com ativos não autorizados devem ser realizados semanalmente, conforme segue:

I - identificação inicial:

a) após a varredura passiva identificar um ativo não autorizado, deve-se registrar imediatamente o dispositivo, coletando informações relevantes, como endereço MAC, IP atribuído, horário de detecção e localização na rede; e

b) verificar se o dispositivo pode ter sido erroneamente classificado como não autorizado, comparando com os registros de manutenção e aprovações recentes.

II - isolamento do dispositivo:

a) o ativo não autorizado deve ser imediatamente isolado da rede para evitar possíveis ameaças ou violações de segurança. Este isolamento pode ser feito automaticamente pela ferramenta de descoberta passiva ou manualmente pela equipe de segurança de TI; e

b) nenhum tráfego adicional de rede deve ser permitido do dispositivo até que seja investigado e validado.

III - notificação e investigação:

a) uma notificação deve ser enviada à equipe de segurança cibernética e ao gestor responsável pela área, relatando o ativo detectado e as ações de isolamento tomadas; e

b) iniciar uma investigação para determinar a origem do dispositivo, incluindo uma consulta ao proprietário potencial e análise de **logs** de rede para rastrear atividades recentes associadas ao ativo.

IV - validação e aprovação:

a) se o dispositivo for identificado como legítimo, mas não autorizado formalmente, o responsável deve seguir o procedimento de regularização, que inclui a revisão de políticas de aprovação de novos dispositivos e sua inclusão no inventário oficial; e

b) se o dispositivo for considerado uma ameaça ou for um equipamento não autorizado sem justificativa, ele deve ser removido permanentemente da rede.

V - documentação e relatório:

a) todas as etapas do processo de identificação, isolamento, investigação e resolução devem ser devidamente documentadas, incluindo o motivo do não reconhecimento inicial do dispositivo e as ações corretivas tomadas; e

b) um relatório semanal deve ser gerado, destacando os dispositivos não autoriza- dos detectados e as medidas de mitigação aplicadas.

VI - ações corretivas - se um ativo não autorizado for detectado repetidamente, um plano de ação corretiva deve ser implementado, que pode incluir revisões nos controles de acesso à rede, auditorias de segurança mais frequentes e treinamento adicional para os responsáveis pelo controle de ativos.

Parágrafo único. Os Elos do STI devem observar se a identificação e endereçamento dos ativos

não autorizados pode envolver intencionalmente ou não a coleta de dados pessoais e tomar medidas de controle adequadas para evitar o vazamento.

Seção III
Da identificação de ativos conectados à rede corporativa

Art. 18. Deve-se utilizar ferramentas de descoberta ativa e passiva e soluções padronizadas, como **logs** de DHCP, para identificar e atualizar continuamente o inventário de ativos conectados à rede corporativa.

Art. 19. A ferramenta de descoberta ativa deve ser executada diariamente ou com mais frequência.

Art. 20. A revisão e atualização do inventário de ativos corporativos deve ocorrer semanalmente ou com mais frequência.

CAPÍTULO III
INVENTÁRIO E CONTROLE DE ATIVOS DE SOFTWARE

Art. 21. Os Elos do STI deverão observar e aplicar as diretrizes a seguir, bem como a Política de Gestão de Ativos estabelecida no Anexo XIV no processo de inventário e controle de ativos de **software**.

Seção I
Do inventário de software

Art. 22. O STI deve estabelecer e manter um inventário detalhado de todos os **softwares** licenciados instalados em ativos corporativos.

Art. 23. O inventário de **software** deve documentar:

I - títulos dos **softwares**;

II - editores dos **softwares**;

III - versão;

IV - data inicial de instalação;

V - uso e objetivo de negócio de cada entrada; e

VI - quando apropriado:

a) **Uniform Resource Locator** (URL);

b) loja de aplicativos;

c) mecanismo de implantação; e

d) data de desativação.

§ 1º Deve ser empregada uma ferramenta de inventário de **software** para automatizar a descoberta e documentação do **software** instalado no âmbito do COMAER.

§ 2º O inventário de **software** deve ser revisado e atualizado semestralmente ou com mais frequência, conforme necessário.

Seção II
Do controle de manutenção de suporte de softwares autorizados

Art. 24. O STI deve manter uma lista de **softwares** autorizados para uso em ativos institucionais, considerando que **softwares** não suportados, sem documentação de exceção, serão designados como não autorizados.

Parágrafo único. **Softwares** sem suporte do fabricante devem ser identificados no sistema de inventário.

Art. 25. Se o **software** não é suportado, mas é necessário para o cumprimento da missão, a exceção deve ser solicitada à DTI com um arrazoado detalhando os controles de mitigação e a aceitação do risco residual, conforme o modelo contido conta no Anexo XXVII (Termo de Exceção Para Uso de Software Sem Suporte).

Art. 26. O inventário de **software** deve ser revisado pelo menos uma vez por mês para verificar o suporte do **software**.

Seção III
Do endereçamento de softwares não autorizados

Art. 27. Os **softwares** não autorizados devem ser retirados de uso em ativos corporativos.

Art. 28. A solicitação de exceção para o uso de **softwares** não autorizados deve conter, no mínimo:

I - identificação completa do solicitante e da unidade responsável;

II - descrição técnica do **software** a ser utilizado, com nome e versão;

III - justificativa detalhada da necessidade operacional ou técnica do **software**;

IV - avaliação de riscos à segurança da informação e as possíveis implicações;

V - medidas de mitigação de riscos que serão adotadas durante o uso;

VI - prazo estimado para o uso da exceção; e

VII - aprovação do Elo Especializado do STI responsável pelo tema.

Parágrafo único. A lista de permissões de **software** deve ser revisada mensalmente, ou com mais frequência, pelo Elo Especializado do STI responsável pelo tema.

Seção IV
Da lista de permissões de software autorizado

Art. 29. O Elo Especializado do STI responsável pelo tema deve manter na página do STI na Intraer um manual de utilização de controles técnicos para garantir que apenas **software** autorizado possa ser executado em ativos institucionais.

Art. 30. Os Elos do STI responsáveis pela gerência de redes devem fazer uso do manual supracitado para garantir que apenas **software** autorizado possa ser executado em ativos institucionais.

Parágrafo único. A lista de permissões de **software** deve ser revisada mensalmente, ou com mais frequência, pelo Elo Especializado do STI responsável pelo tema.

Seção V
Da lista de permissões de bibliotecas autorizadas

Art. 31. O Elo Especializado do STI responsável pelo tema deve disponibilizar na página do STI na Intraer uma lista de bibliotecas de **software** autorizadas, como arquivos .dll, .ocx e .so, que tenham permissão para carregar em um processo do sistema em ativos institucionais.

Parágrafo único. O Elo Especializado do STI responsável pelo tema deve revisar a lista de bibliotecas de **software** autorizadas semestralmente ou com mais frequência.

Art. 32. Os Elos do STI responsáveis por gerência de redes devem seguir estritamente a lista de bibliotecas autorizadas, garantindo que somente essas bibliotecas possam ser carregadas em ativos institucionais.

Art. 33. Os Elo do STI responsáveis por gerência de redes devem impedir que bibliotecas não autorizadas sejam carregadas em um processo do sistema.

Seção VI
Da lista de permissões de Scripts autorizados

Art. 34. O Elo Especializado do STI responsável pelo tema deve disponibilizar na página do STI na Intraer uma lista de **scripts** autorizados, como arquivos .ps1 e .py, que tenham permissão para execução em ativos institucionais. A lista deve incluir o motivo do uso e o impacto esperado de cada **script** nos ativos institucionais.

Art. 35. A execução de **scripts** não autorizados deve ser bloqueada por padrão.

Parágrafo único. O Elo Especializado do STI responsável pelo desenvolvimento deve revisar a lista de **scripts** semestralmente ou com mais frequência.

CAPÍTULO IV
PROTEÇÃO DE DADOS

Seção I
Do processo de gestão e inventário de dados

Art. 36. O processo de gestão de dados no COMAER deve seguir a Política de Gestão de Dados, seu indicador consta no Anexo XV, com manutenção de um inventário atualizado de dados pelo STI.

Parágrafo único. Esse inventário deve ser reavaliado e atualizado anualmente.

Seção II
Das listas de controle de acessos a dados

Art. 37. O STI deve implementar e manter listas de controle de acesso a dados para sistemas de arquivos, bancos de dados e aplicações, em conformidade com padrões de perfis definidos de acordo com a necessidade.

Seção III
Do tratamento seguro de dados

Art. 38. A documentação do fluxo de dados deve ser realizada com base na Política de Gestão de Dados do COMAER, seu indicador consta no Anexo XV. Os padrões de retenção e descarte seguro de dados no COMAER devem seguir as diretrizes estabelecidas, respeitando a sensibilidade das informações.

Parágrafo único. O esquema de classificação deve ser reavaliado e atualizado anualmente ou quando ocorrerem mudanças significativas que possam impactar essa medida de segurança.

Seção IV
Da criptografia dos dados sensíveis

Art. 39. Os padrões para criptografia dos dados sensíveis em trânsito, repouso e em dispositivos de usuário final estão definidos na Instrução Normativa GSI nº 3, 6 de março de 2013 e na Norma Complementar nº 09/IN01/DSIC/GSI/PR, de 15 de julho de 2014, a qual estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.

Seção V
Do registro de acesso a dados sensíveis

Art. 40. Os padrões para o registro do acesso a dados sensíveis, incluindo modificação e descarte, estão definidos na Política de Manipulação de Informações Classificadas (Anexo IV).

Seção VI
Da segmentação do processamento e armazenamento de dados com base na sensibilidade

Art. 41. Os Elos do STI devem segmentar o processamento e armazenamento de dados com base na sensibilidade dos dados.

Parágrafo único. Dados sensíveis não devem ser processados em ativos institucionais destinados a dados de menor sensibilidade.

Seção VII
Da solução de prevenção contra perda de dados

Art. 42. O Órgão Central do STI padronizará a ferramenta para prevenção de perda de dados (DLP) baseada em **host** a ser utilizada no âmbito do COMAER, disponibilizando o manual de operação da ferramenta na página do STI na Intraer.

Art. 43. Os Elos do STI devem utilizar a ferramenta automatizada para identificar todos os dados sensíveis armazenados, processados ou transmitidos por meio de ativos institucionais, conforme manual disponibilizado.

CAPÍTULO V
CONFIGURAÇÃO SEGURA DE ATIVOS INSTITUCIONAIS E SOFTWARE

Art. 44. As diretrizes a seguir aplicam-se a todos os ativos corporativos, incluindo dispositivos de usuário final (portáteis e móveis), dispositivos não computacionais/IoT, servidores, sistemas operacionais e **software** (sistemas operacionais e aplicações).

Art. 45. Os Elos do STI devem ajustar as configurações de segurança de dispositivos e **softwares** sob sua responsabilidade utilizados na organização a fim de proteger a privacidade dos militares, evitando que suas informações sejam expostas ou que suas contas sejam invadidas.

Seção I
Do processo de configuração segura

Art. 46. O processo de configuração segura para ativos corporativos (dispositivos de usuário final, incluindo portáteis e móveis; dispositivos de redes, dispositivos não computacionais/IoT; e servidores) e **software** (sistemas operacionais e aplicações) e seu indicador consta no Anexo XVI.

Art. 47. Os Elos do STI devem revisar e atualizar a documentação da gestão de configuração dos ativos e **softwares** sob sua responsabilidade anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança.

Seção II
Do processo de configuração segura para a Infraestrutura de Rede

Art. 48. Os Elos do STI devem configurar as Infraestruturas de rede do COMAER conforme a Política de Gestão de Ativos, consta no Anexo XIV.

Art. 49. Todo o tráfego de rede deve ser gerenciado por **firewall**, e os Elos do STI devem garantir que os dispositivos estejam configurados com **firewall** ativo, conforme disposto na Política de Segurança dos Serviços de Rede, seu indicador consta no Anexo VIII.

Art. 50. Os Elos do STI devem garantir que todos os dispositivos de usuário final sejam gerenciados por um **firewall** baseado em **host**, conforme Política de Segurança dos Serviços de Rede, consta no Anexo VIII.

Art. 51. Os Elos do STI devem configurar servidores DNS (**Domain Name System**) confiáveis nos ativos corporativos sob sua responsabilidade. Exemplos de implementações incluem a configuração de ativos para usar servidores DNS controlados pelo COMAER.

Art. 52. Os Elos do STI devem implementar um processo contínuo de manutenção das configurações de segurança, incluindo a revisão regular das configurações para garantir que permaneçam em conformidade com as políticas de segurança da organização.

Art. 53. Mudanças nas configurações de segurança devem ser documentadas e aprovadas através de um processo formal de gerenciamento de mudanças.

Parágrafo único. O Órgão Central do STI deve revisar e atualizar a documentação desse processo anualmente ou quando ocorrerem mudanças significativas que possam impactar esta medida de segurança, como a introdução de novas tecnologias, alterações na estrutura da rede, ou mudanças nos requisitos de segurança, a documentação deve ser revisada e ajustada de imediato para refletir essas alterações e garantir que a segurança da rede não seja comprometida.

Seção III
Do gerenciamento seguro de ativos corporativos e softwares

Art. 54. Os administradores de sistemas e os Elos do STI devem gerenciar de forma segura os ativos e **softwares** sob sua responsabilidade, adotando controle de versões documentado (snapshots), infraestrutura de código versionada (**version controlled-infrastructure-as-code**) e acesso a interfaces administrativas por protocolos seguros, conforme a Política de Administração de Recursos Computacionais, seu indicador consta no Anexo III.

Art. 55. Cabe ao Elo do STI gerenciar o bloqueio automático de dispositivos por inatividade de acordo com o previsto na Política de Administração de Recursos Computacionais, consta no Anexo III.

Art. 56. O Elo do STI deve implementar a capacidade de limpeza remota de dados corporativos em dispositivos portáteis, aplicando-a em casos de perda, roubo ou desligamento do usuário. O usuário deve preencher o Termo de Autorização para Limpeza Remota De Dados Em Dispositivos Portáteis, seu indicador consta no Anexo XXVIII, concordando com a possibilidade de limpeza remota dos dados.

Art. 57. O Elo do STI deve assegurar a separação dos espaços de trabalho nos dispositivos móveis, criando perfis separados para dados corporativos e pessoais. Práticas recomendadas incluem:

I - configurar e gerenciar perfis de trabalho;

II - implementar políticas que restrinjam o acesso a dados corporativos somente no perfil corporativo; e

III - monitorar a conformidade com as políticas de separação de dados.

Seção IV
Do gerenciamento de contas padrão em ativos corporativos e softwares

Art. 58. Os Elos do STI devem gerenciar contas padrão nos ativos e **softwares** corporativos sob sua responsabilidade, como root, administrador e outras contas de fornecedores pré-configuradas. Exemplos de implementações podem incluir:

I - desativar ou alterar as credenciais das contas padrão para evitar que sejam exploradas por atacantes;

II - tornar contas padrão inutilizáveis ou substituí-las por contas com credenciais personalizadas e seguras; e

III - monitorar e auditar o uso dessas contas para garantir que práticas seguras estejam sendo seguidas.

Seção V
Da remoção ou desativação de serviços desnecessários nos ativos e software

Art. 59. Os Elos do STI são responsáveis por desinstalar ou desativar serviços desnecessários nos ativos e **softwares** corporativos sob sua responsabilidade, como um serviço de compartilhamento de arquivos não utilizado, módulo de aplicação da web ou função de serviço.

Art. 60. Os Elos do STI devem auxiliar na identificação de serviços que representam riscos e na definição de políticas para garantir que apenas os serviços necessários estejam ativos, como:

I - identificar serviços não essenciais ou não utilizados que possam representar riscos de segurança;

II - desativar ou remover esses serviços para reduzir a superfície de ataque e melhorar o desempenho e a segurança dos sistemas; e

III - manter a documentação de quais serviços foram desativados ou removidos e garantir que o ambiente de TI esteja configurado conforme as necessidades da organização.

Seção VI
Das responsabilidades

Art. 61. Em todas as Organizações Militares os Comandantes, Chefes ou Diretores são responsáveis por garantir a correta configuração e manutenção segura de todos os ativos corporativos e **software** sob sua competência.

Art. 62. O Órgão Central do STI deve aprovar qualquer mudança significativa na configuração e assegurar que a documentação seja atualizada conforme necessário.

CAPÍTULO VI
GESTÃO DE CONTAS

Art. 63. Os procedimentos e atividades relativos à gestão de contas definidos neste capítulo devem ser revisados e executados, no mínimo, trimestralmente, conforme as diretrizes

Art. 64. Os Elos de Serviço do STI devem utilizar um serviço de diretório ou identidade, assegurando controle unificado e seguro para manter um inventário atualizado e centralizado de todas as contas, incluindo usuários, administradores e contas de serviço, validando a autorização, no mínimo, trimestralmente, de acordo com as orientações da Política de Administração de Recursos Computacionais (Anexo III).

Parágrafo único. Preferencialmente, caso possível, essa função deve ser exercida por um Elo Especializado no tema, garantindo maior segurança e controle sobre as contas gerenciadas.

Art. 65. O Elo de Serviço do STI deve utilizar senhas únicas para cada ativo, devendo permanecer alinhadas aos requisitos contidos na Política de Uso de Recursos Computacionais (Anexo III).

Parágrafo único. Deverá ser implementado senhas seguindo a recomendação de uso do MFA para acessos internos e a obrigatoriedade do MFA ou SSO (**Single Sign- On**) para acessos externos via Internet.

Art. 66. Os Elos de Serviço do STI devem desativar contas inativas conforme as diretrizes da Política de Administração de Recursos Computacionais (Anexo III).

Seção I
Da limitação de privilégios de administrador a contas de administrador dedicadas

Art. 67. Os Elos de Serviço do STI devem restringir os privilégios de administrador às contas de administrador dedicadas nos ativos institucionais. Atividades gerais de computação, como navegação na Internet, **e-mail** e uso do pacote de produtividade, devem ser realizadas a partir da conta primária não privilegiada do usuário, conforme estipulado no Anexo III desta norma.

Art. 68. Para assegurar um ambiente controlado e seguro na realização de tarefas administrativas e gerais, a gestão de contas privilegiadas deve seguir as diretrizes estabelecidas nos procedimentos de segurança, incluindo a implementação de políticas de controle de acesso, monitoramento de contas e auditorias periódicas, conforme orientado na Política de Uso de Recursos Computacionais (Anexo II).

Art. 69. A implementação de soluções de segurança e a proteção de contas devem seguir as diretrizes estabelecidas na Política de Segurança Lógica (Anexo XI) e na Política de Backup e Restauração de Dados Digitais (Anexo XIII) para assegurar a integridade e a proteção de dados.

CAPÍTULO VII
GESTÃO DO CONTROLE DE ACESSO

Art. 70. Os Elos de Serviço do STI são responsáveis por criar, atribuir, gerenciar e revogar credenciais de acesso e privilégios para contas de usuário, serviço e administrador para ativos e **softwares** corporativos, anualmente.

Seção I
Do processo de concessão de acesso

Art. 71. Os Elos de Serviço do STI deverão estabelecer processos de concessão de acesso de forma padronizada, preferencialmente baseado em funções.

Seção II
Do processo de revogação de acesso

Art. 72. Os Elos de Serviço do STI deverão estabelecer processos de revogação de acesso de forma automatizada e padronizada.

Parágrafo único. Tal processo deve garantir que os acessos sejam removidos de maneira eficiente, especialmente quando um militar deixa a OM ou mudar de função. Em alguns casos, o gestor direto do militar também pode ser responsável por iniciar o processo de revogação de acesso.

Seção III
Da utilização de MFA

Art. 73. Os sistemas com acesso externo deverão utilizar MFA ou SSO (**Single Sign- On**) para as aplicações, conforme Anexo II.

Art. 74. O uso de MFA é obrigatório para o acesso remoto à Intraer (VPN).

Art. 75. Todas as contas de administrador deverão exigir MFA para realizar o acesso. É de responsabilidade do Órgão Central do STI garantir e auditar a utilização de MFA para contas de administrador. Cabe aos Elos Especializados configurarem as políticas de segurança e assegurar a proteção de acessos administrativos.

Seção IV
Do inventário de sistemas de autenticação e autorização

Art. 76. O Elo do STI responsável deverá manter um inventário dos sistemas de autenticação e autorização.

Parágrafo único. O inventário deverá ser revisado e atualizado anualmente ou com mais frequência.

Seção V
Do controle de acesso baseado em funções

Art. 77. O controle de acesso baseado em funções (RBAC) deve ser implementado para garantir que os usuários tenham os privilégios adequados de acordo com suas funções na organização, conforme Política de Gestão de Dados (Anexo XV).

Seção VI
Do controle de acesso físico

Art. 78. As instalações que hospedam sistemas de TI devem ter seu acesso controlado e restrito aos elementos devidamente autorizados, a fim de garantir a integridade, a confidencialidade e a disponibilidade das informações. Estas instalações deverão ser providas de sistemas de acesso baseadas no uso de biometria e de circuito fechado de câmeras, devendo o registro dos acessos permanecer arquivado por no mínimo 90 dias.

Art. 79. O controle de acesso físico no COMAER deve ser realizado conforme estabelecido na Política de Controle de Acesso (Anexo XVI).

Seção VII
Do controle de acesso lógico

Art. 80. O acesso lógico aos sistemas de TI deve ser protegido por meio das medidas dedicadas de segurança, tais como senhas seguras ou, quando necessário, de dispositivos de segurança adicionais, tais como **smart cards**, **tokens** e interfaces com biometria.

Art. 81. Os usuários de sistemas de TI devem preservar a confidencialidade de suas senhas pessoais de acesso aos sistemas e, consequentemente, responder por todos os atos praticados utilizando as senhas em questão.

Art. 82. A necessidade de utilização de dispositivos de segurança adicionais, tais como **smart cards**, **tokens** e interfaces com biometria, ficará sujeita à avaliação por parte do CIAER, mediante solicitação direta do Comandante, Chefe ou Diretor da OM.

Art. 83. É desejável que o acesso a serviços ou sistemas pela Intraer utilize múltiplos fatores de autenticação, ou MFA, como medida adicional de segurança.

Art. 84. O acesso a serviços ou sistemas por meio da Internet deve obrigatoriamente implementar MFA, como forma de incrementar a segurança da aplicação e reduzir os riscos associados ao comprometimento de credenciais de acesso de militares e servidores civis da Força Aérea.

Art. 85. O controle de acesso lógico no COMAER deve ser realizado conforme estabelecido na Política de Controle de Acesso (Anexo XVI).

CAPÍTULO VIII
GESTÃO CONTÍNUA DE VULNERABILIDADES

Seção I
Do processo de gestão de vulnerabilidade

Art. 86. Os Elos Especializados deverão manter um processo de gestão de vulnerabilidades documentado para ativos corporativos.

Art. 87. Parágrafo único. A documentação deve ser revisada anualmente ou sempre que ocorrerem mudanças significativas que possam impactar esta medida de segurança.

Art. 88. Os Elos Especializados deverão rastrear e avaliar vulnerabilidades nos ativos corporativos do COMAER, em seu escopo de atuação, realizando varreduras automatizadas trimestrais em ativos internos e mensais em ativos externos, seguindo o padrão SCAP (**Security Content Automation Protocol**).

Art. 89. Compete ao Elo Especializado responsável por Segurança da Informação monitorar fontes públicas e privadas para novas informações sobre ameaças e vulnerabilidades.

Art. 90. Os Elos de Serviço do STI deverão possuir uma gestão automatizada de **patches** para atualizações de forma centralizada, atualizado mensalmente.

Seção II
Do processo de remediação

Art. 91. O Elo Especializado responsável por Segurança da Informação deverá informar ao responsável pelos ativos institucionais sobre as vulnerabilidades.

Art. 92. É de responsabilidade do mantenedor dos ativos institucionais corrigir as vulnerabilidades informadas pelo Elo Especializado e manter atualizados os **patches** de segurança, bem como os **patches** de aplicações e dos sistemas operacionais.

Art. 93. O Elo Especializado responsável por Segurança da Informação deverá revisar as remediações das vulnerabilidades baseada na classificação de riscos.

Parágrafo único. As revisões deverão ser realizadas mensalmente.

CAPÍTULO IX
GESTÃO DE REGISTROS DE AUDITORIA

Seção I
Do processo de gestão de log de auditoria

Art. 94. Os processos de coleta, armazenamento, retenção e armazenamento de **logs** em ativos corporativos no âmbito do COMAER devem observar o exposto na Política de Gestão de Registros (**Logs**) de Auditoria – PGRA (Anexo XVII).

Parágrafo único. A referida Política deve ser revisada anualmente ou sempre que ocorrerem

mudanças significativas que possam impactar esta medida de segurança.

CAPÍTULO X
PROTEÇÕES DE E-MAIL E NAVEGADOR WEB

Seção I
Do uso de serviços de filtragem de DNS

Art. 95. Todos os ativos corporativos devem utilizar os serviços de filtragem de DNS fornecidos pelos Elos Especializados do STI para bloquear o acesso a domínios mal-intencionados conhecidos.

Seção II
Da imposição de filtros de URL baseados em rede

Art. 96. Os Elos Especializados deverão utilizar filtros de URL baseados em rede que devem ser aplicados para limitar os ativos corporativos de se conectarem a sites potencialmente maliciosos ou não aprovados.

§ 1º As implementações incluem filtragem baseada em categoria, filtragem baseada em reputação ou através do uso de listas de bloqueio.

§ 2º Esses filtros devem ser aplicados a todos os ativos corporativos para garantir proteção contínua contra sites indesejados.

Seção III
Da restrição a ferramentas desnecessárias ou não autorizadas

Art. 97. A utilização de ferramentas de navegação e extensões de navegador deve ser estritamente controlada pelo Elo do STI, responsável por garantir a integridade da rede corporativa e a segurança dos ativos, conforme descrito na Política de Administração de Recursos Computacionais (Anexo III).

Seção IV
Da implementação do DMARC

Art. 98. O Elo do STI administrador do serviço de e-mail corporativo deve implementar a política e verificação DMARC (**Domain-based Message Authentication, Reporting & Conformance**) para reduzir a chance de **e-mails** forjados ou modificados provenientes de domínios válidos. Isso inclui a configuração dos padrões SPF (**Sender Policy Framework**) e DKIM (**DomainKeys Identified Mail**), garantindo a autenticação dos **e-mails** enviados e recebidos.

Seção V
Do bloqueio de tipos de arquivo desnecessários

Art. 99. O Elo do STI administrador do serviço de **e-mail** corporativo deve configurar o **gateway** de **e-mail** para bloquear tipos de arquivo desnecessários à utilização do **e-mail**.

Seção VI
Das proteções anti-malware de servidor de e-mail

Art. 100. O Elo do STI administrador do serviço de e-mail corporativo deve manter proteção **anti-malware** nos servidores de **e-mail**, incluindo a varredura de anexos e/ou o uso de **sandbox**. Essa proteção deve identificar e neutralizar ameaças antes que possam comprometer a segurança dos servidores e a integridade das comunicações.

CAPÍTULO XI
DEFESAS CONTRA MALWARE

Seção I
Do software anti-malware

Art. 101. Deverão ser instalados e configurados, pelos Elos de Serviço, nos equipamentos, servidores e nas estações de trabalho de TI, o **software** antivírus corporativo e outros utilitários indicados pelo Órgão Central do STI para prevenir ou mitigar ataques gerados por programas maliciosos.

§ 1º Deverão ser habilitados os recursos anti-exploração em ativos e **softwares** corporativos do COMAER, onde possível.

§ 2º O Órgão Central do STI é responsável por padronizar o **software** de antivírus corporativo.

§ 3º Os setores de TI das OM poderão adquirir produtos distintos do padronizado, desde que autorizado pelo respectivo ODGSA e pelo Órgão Central do STI.

Art. 102. O **software anti-malware** deverá obter atualizações automáticas para arquivos de assinatura **anti-malware** em todos os ativos corporativos.

Art. 103. O **software anti-malware** deverá realizar análise comportamental para detectar e bloquear comportamentos anômalos que indiquem a presença de **malware**.

Seção II
Da reprodução automática para mídias removíveis

Art. 104. É vedada a reprodução automática de mídias removíveis em todos os dispositivos e sistemas da organização.

Parágrafo único. Os elos do STI responsáveis por gerência de redes devem garantir que essa configuração esteja parametrizada por padrão nas estações de trabalho em sua área de atuação.

Seção III
Da varredura anti-malware automática de mídias removíveis

Art. 105. É obrigatória a realização de varredura automática em todas as mídias removíveis antes de qualquer acesso ou operação, visando identificar e neutralizar possíveis ameaças e garantir a segurança dos dados e sistemas corporativos.

Seção IV
Da centralização do gerenciamento do software anti-malware

Art. 106. O gerenciamento do **software anti-malware** deverá ser centralizado pelo Elo Especializado.

Parágrafo único. A instalação e a gestão dos servidores secundários de **software anti-malware** são de responsabilidade dos Elos de Serviço do STI.

Seção V
Dos serviços de mensagem instantânea

Art. 107. É vedada a utilização de serviços de mensagem instantânea (chat ou bate-papo) que trafeguem informações pela Internet (hospedados e mantidos por entidades externas ao COMAER), por estes serem, comprovadamente, grandes difusores de programas maliciosos, cabendo ao Chefe do Elo de Serviço de TI a responsabilidade pelo cumprimento deste item.

Parágrafo único. Os Comandantes, Chefes ou Diretores de OM poderão autorizar excessões, assumindo a responsabilidade pelos riscos, conforme procedimentos descritos em ato normativo do STI sobre o Uso das Rede de Dados no COMAER.

Art. 108. Está autorizado o uso de serviços de mensagem instantânea (chat ou bate-papo), de âmbito interno da Organização (rede local) ou entre Organizações (Intraer), exclusivamente para uso institucional, hospedados e mantidos pela OM, desde que se utilizem de **softwares** homologados divulgados na página do Órgão Central do STI na Intraer.

CAPÍTULO XII
RECUPERAÇÃO DE DADOS

Seção I
Do processo de recuperação de dados

Art. 109. Os Elos do STI que realizarem gestões de dados devem estabelecer e manter um processo formal de recuperação de dados, abrangendo todo o escopo das atividades, como, por exemplo, os **backups** de qualquer origem, que devem ser devidamente registrados, controlados e protegidos.

Parágrafo único. A documentação do processo de recuperação de dados deve ser revisada e atualizada anualmente.

Seção II
Da execução de backups automatizados

Art. 110. Deverão ser realizados **backups** automatizados de ativos corporativos.

Parágrafo único. Os **backups** automatizados devem ser realizados em horários de menor tráfego de rede para minimizar o impacto no desempenho dos sistemas. Sempre que possível, recomenda-se a aplicação de técnicas de compressão de dados, de forma a reduzir o tráfego e otimizar o uso da largura de banda durante o processo de **backup**.

Seção III
Da proteção aos dados de recuperação

Art. 111. Os Elos de Serviço do STI deverão proteger os dados de recuperação com controles equivalentes aos dados originais. Deve ser observado o uso de criptografia e separação dos dados com base nos requisitos levantados no processo de recuperação dos dados.

Parágrafo único. A documentação do processo de recuperação deve ser revisada anualmente ou sempre que ocorrerem mudanças significativas que possam impactar esta medida de segurança.

Seção IV
Do estabelecimento e manutenção de instância isolada de dados de recuperação

Art. 112. Os sistemas devem possuir uma instância isolada dos dados de recuperação, localizada em um data center separado para garantir maior segurança e disponibilidade.

Seção V
Do teste dos dados de recuperação

Art. 113. A recuperação de dados deverá ser testada trimestralmente para garantir que os **backups** e os sistemas de recuperação estão operacionais e prontos para uso em caso de necessidade.

CAPÍTULO XIII
GESTÃO DA INFRAESTRUTURA DE REDE

Art. 114. Os Elos de Serviço do STI devem estabelecer, implementar e gerenciar ativamente (rastrear, reportar, corrigir) os dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

Art. 115. Os Elos de Serviço do STI devem manter uma rede segura para proteger contra ataques, garantindo a configuração correta de dispositivos como roteadores e **firewalls**, pois as configurações padrão desses dispositivos não são focadas em segurança.

Parágrafo único. As configurações de rede devem ser revisadas e atualizadas regularmente para evitar falhas exploráveis e garantir que exceções antigas sejam removidas.

Seção I
Da garantia de atualização da infraestrutura de rede

Art. 116. Os Elos de Serviço do STI deverão garantir que a infraestrutura de rede seja mantida atualizada, utilizando a versão mais recente do **software** ou adotando ofertas de NaaS (**Network-as-a-Service**) suportadas e revisando as versões do **software** mensalmente, ou com mais frequência, a fim de verificar o suporte do **software**.

Seção II
Da garantia de níveis de segurança para a arquitetura de rede

Art. 117. Os Elos de Serviço do STI devem estabelecer e manter uma arquitetura de rede segura, sob sua responsabilidade, que aborda os princípios de segmentação, privilégio mínimo e disponibilidade.

Seção III
Do gerenciamento da infraestrutura de rede e segurança

Art. 118. Os Elos de Serviço do STI deverão assegurar que a infraestrutura de rede seja mantida atualizada, revisando o **software** mensalmente para garantir o suporte contínuo.

Seção IV
Dos diagramas de arquitetura

Art. 119. Os Elos de Serviço do STI deverão elaborar e manter diagramas de arquitetura de rede, ou outra documentação similar, com revisões anuais ou sempre que houver mudanças significativas na estrutura de rede.

Seção V
Da centralização da Autenticação, Autorização e Auditoria de rede (AAA)

Art. 120. Os Elos Especializados devem manter o processo de AAA de forma que seja centralizado, facilitando a gestão e assegurando uma aplicação consistente das regras de segurança. A centralização do AAA permitirá a detecção e resposta eficiente a atividades suspeitas. Esse processo deverá abordar, no mínimo:

a) autenticação: verificar a identidade dos usuários que tentam acessar a rede, garantindo que apenas indivíduos autorizados tenham acesso. exemplos incluem o uso de nome de usuário e senha, biometria, ou outros fatores de autenticação;

b) autorização: definir as permissões de cada usuário autenticado, determinando quais recursos e serviços podem ser acessados, de acordo com seu perfil e função na organização; e

c) auditoria: monitorar e registrar todas as atividades realizadas na rede, possibilitando a revisão das ações por administradores de rede, com o objetivo de garantir a segurança e a conformidade com as políticas institucionais.

Seção VI
Dos recursos cibernéticos dedicados para trabalhos administrativos

Art. 121. Os Elos de Serviço deverão habilitar a coleta de tráfego de rede e registros de **log** em todos os dispositivos utilizados na execução de tarefas administrativas. Além disso, é obrigatório o uso de recursos cibernéticos dedicados, os quais devem estar fisicamente ou logicamente separados da rede primária da organização e devidamente protegidos. Esses recursos devem ser isolados da rede externa, garantindo a segurança e a segregação apropriada.

Seção VII
Dos serviços de rede da Intraer e da Internet

Art. 122. Os serviços de rede da Intraer e da Internet, disponibilizados pelas OM, deverão ser utilizados somente para apoio às atividades de interesse do COMAER.

Art. 123. Os Elos do STI devem negar o acesso aos serviços de rede da Intraer e da Internet quando os mesmos envolverem procedimentos suspeitos que contrariem as leis em vigor no país ou a moral e os bons costumes, ou que venham a prejudicar a realização das atividades de interesse do COMAER, ou que provoquem danos à imagem do COMAER e das demais instituições governamentais, ou, ainda, que causem prejuízos morais ou financeiros a terceiros.

Art. 124. A entrada em operação de soluções ou serviços de TI que façam uso de recursos da Intraer ou da Internet somente poderá ocorrer a partir de aprovação prévia do Órgão Central do STI.

Art. 125. É proibida a implantação nas redes locais que integram a Intraer de soluções de TI e demais serviços de rede, cuja operação venha a impactar de maneira efetiva o acesso a sistemas de TI de interesse do COMAER ou da Administração Federal, mesmo que os sistemas impactantes sejam restritos ao âmbito da rede local de sua implantação.

Art. 126. A instalação de um acesso remoto à Intraer, qualquer que seja o local da implantação, só poderá ocorrer a partir de aprovação prévia do Órgão Central do STI.

Art. 127. A entrada em operação de acessos dedicados à Internet que venham a ser implantados nas Organizações do COMAER só deverá ocorrer a partir de aprovação prévia do Órgão Central do STI.

Art. 128. A Organização Militar que porventura originar a difusão de vírus ou outro tipo de ameaça eletrônica na Intraer terá o seu acesso bloqueado à Rede de Dados do Comando da Aeronáutica, por determinação do Órgão Central do STI.

Parágrafo único. O Órgão Central do STI também entrará em contato com a Organização orientando, caso julgue conveniente, seu Comandante, Chefe ou Diretor a instaurar sindicância para apuração de autoria e enviará equipe especializada para auxiliar nos trabalhos de investigação de danos e autoria, bem como na eliminação da ameaça.

Seção VIII
Da computação móvel

Art. 129. A utilização de computadores portáteis será precedida de medidas que visem à orientação dos usuários dos equipamentos e, se necessário, do emprego de soluções de criptografia de dados, respeitando normativas gerenciais e técnicas existentes no COMAER.

Art. 130. É vedada a utilização de computadores pessoais (particulares) na rede física das organizações do COMAER.

Parágrafo único. Os Comandantes, Chefes ou Diretores poderão autorizar o uso de computadores pessoais nas redes físicas locais, desde que expressamente autorizado pelo respectivo ODGSA.

CAPÍTULO XIV
MONITORAMENTO E DEFESA DA REDE

Seção I
Da centralização de alertas de eventos de segurança

Art. 131. Os Elos de Serviço devem enviar para as respectivas ETIR de referência os registros de eventos dos ativos de informação sob sua responsabilidade.

Art. 132. O CTIR e as ETIR devem centralizar os alertas de eventos de segurança em ativos institucionais, utilizando soluções como SIEM (**Security Information and Event Management**) para correlação de eventos. Suas tarefas principais devem incluir:

I - a centralização dos alertas de diferentes dispositivos e sistemas;

II - a utilização de **SIEM** para correlacionar eventos e identificar ameaças;

III - a análise regular de **logs** para detectar padrões de comportamento; e

IV - a configuração de alertas relevantes para a Ptç Ciber.

Seção II
Das soluções de detecção de intrusão baseada em host

Art. 133. Os Elos do STI devem implantar soluções para detecção de intrusão baseada em **host.**

Seção III
Das soluções de detecção de intrusão baseada em rede

Art. 134. Os Elos de Serviço devem implementar soluções de detecção de intrusão de rede.

Seção IV
Da filtragem de tráfego entre os segmentos de rede

Art. 135. Cada Elo de Serviço do STI é responsável por configurar a filtragem de tráfego entre os segmentos de rede sob sua responsabilidade, a Intraer e a Internet.

Seção V
Do gerenciamento de controle de acesso em ativos remotos

Art. 136. Os Elos de Serviço do STI devem aplicar o gerenciamento de controle de acesso em ativos sob sua responsabilidade que se conectam remotamente à organização, assegurando que os procedimentos de acesso remoto estejam em conformidade com as disposições previstas na ICA 7-61/2024 – Uso das Redes de Dados no COMAER (Intraer e Internet).

Art. 137. Os Elos de Serviço do STI devem aplicar o gerenciamento de controle de acesso em ativos que se conectam remotamente às OM sob sua responsabilidade, assegurando que sejam:

I - determinadas as quantidades de acesso aos recursos da OM, utilizando **software anti-malware** devidamente atualizado;

II - implementados processos de configuração segura de ativos; e

III - sempre atualizados os sistemas operacionais e demais aplicações.

Seção VI
Da coleta de logs e tráfego de rede

Art. 138. Cabe aos Elos do STI realizar a coleta dos **logs** e tráfego de rede com o objetivo de checar, alertar e tomar providências sobre dispositivos de rede sob sua responsabilidade que estejam com comportamento que fujam do padrão.

Art. 139. Os requisitos que garantem a execução da tarefa de maneira eficiente e segura estão descritos na Política de Gestão de Registros (**Logs**) de Auditoria – PGRA (Anexo XVII).

Seção VII
Das soluções para prevenção de intrusão baseada em host

Art. 140. Cabe aos Elos Especializados implantarem uma solução de prevenção de intrusão baseada em **host** nos ativos institucionais, preferencialmente com suporte do fornecedor.

Seção VIII
Das soluções para prevenção de intrusão de rede

Art. 141. O Órgão central do STI deve definir uma solução para prevenção de intrusão baseada em rede, preferencialmente com suporte do fornecedor, de acordo com a necessidade.

Seção IX
Do controle de acesso ao nível de porta

Art. 142. Os Elos de Serviço do STI devem implementar o controle de acesso ao nível de porta nos ativos sob sua responsabilidade, utilizando o protocolo 802.1x ou soluções semelhantes, como certificados e ferramentas de autenticação de usuário ou dispositivo.

Seção X
Da filtragem de camada de aplicação

Art. 143. Os Elos de Serviço do STI devem implementar mecanismos de filtragem de camada de aplicação, tais como proxy de filtragem, **firewall** de aplicação ou **gateway**, nos ativos sob sua responsabilidade.

Seção XI
Dos limites de alertas de eventos de segurança

Art. 144. Os Elos de Serviço do STI devem ajustar periodicamente os limites dos alertas de eventos de segurança sob sua responsabilidade, garantindo uma rápida detecção de ameaças.

CAPÍTULO XV
CONSCIENTIZAÇÃO E TREINAMENTO DE COMPETÊNCIAS SOBRE SEGURANÇA

Seção I
Do programa de conscientização de segurança

Art. 145. O Elo Especializado responsável por Segurança da Informação deverá apoiar a criação e manutenção de um programa de conscientização básico de segurança, que todos os membros da Força realizem, visando a compreensão dos conhecimentos e comportamentos necessários a fim de garantir a segurança da instituição.

Art. 146. Neste treinamento deverá haver foco na:

I - conscientização sobre os riscos associados ao uso de redes inseguras para a conexão e transmissão de dados institucionais, bem como as melhores práticas para mitigar esses riscos, conforme os conceitos e diretrizes da ICA 7-61/2024;

II - conscientização sobre a importância de habilitar e utilizar as melhores práticas de autenticação segura, como a autenticação de múltiplos fatores, ou MFA, composição de senha e gestão de credenciais;

III - conscientização sobre práticas de mesa e tela limpas, como não deixar senhas expostas e bloquear a tela da estação de trabalho ao se ausentar;

IV - conscientização sobre causas de exposições de dados não intencionais, como perda de dispositivos móveis ou envio incorreto de **e-mails** devido ao preenchimento automático.

V - identificação dos indicadores mais comuns de um incidente e relatar tal incidente imediatamente, seguindo os protocolos estabelecidos;

VI - identificação, armazenagem, transferência, arquivamento e destruição de informações sensíveis (incluindo dados pessoais) de maneira adequada;

VII - identificação de diferentes formas de ataques de engenharia social, como **phishing**, golpes de telefone e chamadas realizadas por impostores.

Seção II
Da conscientização de usuários na identificação e comunicação de ativos institucionais desatualizados em relação à segurança

Art. 147. Todo COMAER deve ser conscientizado sobre a importância de comunicar ativos institucionais desatualizados ou vulneráveis no contexto de segurança. As seguintes diretrizes devem ser seguidas:

I - conscientização sobre identificação de ativos desatualizados:

a) conscientizar os militares para reconhecer sinais de que ativos, como **software** ou sistemas operacionais, estão desatualizados e podem representar riscos de segurança; e

b) incluir a importância de manter os ativos atualizados para prevenir ataques baseados em vulnerabilidades conhecidas.

II - procedimento de comunicação:

a) relatar ativos desatualizados ou obsoletos ao respectivo Elo de Serviço por meio do Sistema de Atendimento ao Usuário (SAU); e

b) garantir que cada comunicação recebida seja registrada e acompanhada até sua resolução, com prazos definidos para resposta.

III - aplicar as sugestões dos relatórios de ativos desatualizados emitidos pelo CTIR.FAB ou ETIR de referência para identificar padrões ou áreas críticas que possam necessitar de uma abordagem mais proativa de atualização e gestão de ativos.

CAPÍTULO XVI
GESTÃO DE PROVEDOR DE SERVIÇOS

Seção I
Do inventário de provedores de serviços

Art. 148. Os Elos do STI deverão criar e gerenciar o inventário de provedores de serviços sob sua responsabilidade, listando todos os provedores da organização. O inventário deve incluir classificações e contatos institucionais para cada provedor de serviço.

Parágrafo único. O inventário deve ser revisado anualmente ou sempre que ocorrerem mudanças significativas que possam impactar a organização de forma relevante.

Seção II
Da política de gestão de provedores de serviços

Art. 149. O Órgão Central do STI deverá criar e gerenciar uma política que aborda a classificação, inventário, avaliação, monitoramento dos provedores de serviço, bem como o encerramento dos seus contratos.

Art. 150. A classificação dos provedores será feita com base nas seguintes características:

I - sensibilidade dos dados;

II - volume de dados;

III - requisitos de disponibilidade; e

IV - classificação de risco.

CAPÍTULO XVII
SEGURANÇA DE APLICAÇÕES

Seção I
Do processo de desenvolvimento seguro de aplicações

Art. 151. O Elo Especializado deverá estabelecer e manter um processo de desenvolvimento seguro de aplicações, devendo tratar de itens como padrões de design seguro de aplicações (**Security by Design**), práticas de codificação seguras, treinamentos para desenvolvedores, gestão de vulnerabilidades, segurança de código de terceiros e procedimentos de teste de segurança de aplicação.

Parágrafo único. O Órgão Central do STI definirá os padrões mínimos para desenvolvimento seguro em ato normativo específico.

Art. 152. Deverá ser realizada uma revisão e/ou alteração do processo periodicamente, em casos específicos ou quando ocorrerem mudanças na organização que venham impactar significativamente.

Art. 153. O Elo Especializado deve gerenciar o ciclo de vida da segurança do **software** desenvolvido, hospedado ou adquirido, prevenindo e corrigindo vulnerabilidades que possam comprometer a instituição.

Seção II
Do processo de aceitação e tratamento de vulnerabilidades de software

Art. 154. O Elo Especializado deverá estabelecer e manter um processo de aceitação e tratamento de informações sobre vulnerabilidades de **softwares**, incluindo mecanismos padronizados de comunicação das vulnerabilidades ao setor responsável. O processo deve incluir políticas de tratamento de vulnerabilidades identificadas, equipe ou profissional responsável por analisar relatórios e um procedimento para entrada, atribuição, correção e testes.

Art. 155. As vulnerabilidades devem ser rastreadas, classificadas quanto à gravidade, e ser atribuídas métricas para medir o tempo de identificação, análise e correção. Revisões periódicas do processo devem ser realizadas, especialmente em casos de mudanças significativas na organização. Quando a correção não for possível, o risco deverá ser gerenciado conforme previsto nesta Política.

Art. 156. Executar a análise de causa raiz em vulnerabilidades de segurança para identificar os problemas subjacentes que criam falhas no código, permitindo que as equipes de desenvolvimento atuem além da correção de vulnerabilidades individuais e evitando a recorrência de problemas semelhantes.

Art. 157. Estabelecer e manter um processo para a classificação de gravidade de vulnerabilidades, facilitando a priorização conforme as vulnerabilidades são corrigidas. Tal processo deve definir um nível mínimo de aceitabilidade de segurança para a liberação de código ou aplicações. A classificação de gravidade deve permitir a triagem sistemática de vulnerabilidades, melhorando a gestão de riscos e garantindo que os bugs mais críticos sejam priorizados.

§ 1º É imprescindível que os riscos e seus fatores, como valores dos ativos, consequências, vulnerabilidades e probabilidades, sejam monitorados e analisados criticamente e continuamente a fim de se identificar o mais rápido possível quaisquer eventuais mudanças no contexto da Organização.

§ 2º O processo de gestão de riscos permite identificar os riscos que podem causar impacto negativo nas atividades operacionais e administrativas do STI, de acordo com a Norma ABNT ISO/IEC 27005:2023.

Parágrafo único. O processo e a classificação de vulnerabilidades devem ser revisados periodicamente.

Seção III
Do inventário de componentes de software de terceiros

Art. 158. O Elo Especializado deverá estabelecer e gerenciar um inventário atualizado de componentes de terceiros usados no desenvolvimento, incluindo riscos que possam representar à organização, devendo ser revisado periodicamente para identificar mudanças ou atualizações e validar sua compatibilidade.

Art. 159. O Elo Especializado deverá utilizar apenas componentes de terceiros que sejam atualizados e confiáveis, preferencialmente bibliotecas e estruturas pré-estabelecidas que ofereçam segurança adequada, devendo ser adquiridos de fontes confiáveis ou passar por avaliação de vulnerabilidades antes de serem usados.

Seção IV
Dos modelos de configurações de segurança para infraestrutura de aplicações

Art. 160. O Elo Especializado deverá utilizar modelos de configuração **Security by Default** recomendados pela equipe de segurança para componentes de infraestrutura de aplicações, como servidores subjacentes, bancos de dados e servidores web.

Parágrafo único. O Órgão Central do STI deve emitir normativo abordando os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem, conforme

legislação vigente sobre o assunto do Governo Federal.

Seção V
Da separação de ambientes de produção e homologação

Art. 161. O Elo Especializado do STI deverá manter ambientes separados para sistemas de produção e homologação em ativos sob sua responsabilidade.

Seção VI
Do treinamento de desenvolvedores em conceitos de segurança de aplicações e codificação segura

Art. 162. O gestor do Elo Especializado que realiza desenvolvimento de **software** deve garantir que os desenvolvedores recebam treinamento regular para escrever código seguro, adaptado ao seu ambiente de desenvolvimento e responsabilidades.

Parágrafo único. O treinamento deve cobrir princípios gerais de segurança e práticas padrão de segurança para aplicações, promovendo uma cultura de segurança contínua entre os desenvolvedores.

Seção VII
Da aplicação de princípios de design seguro em arquiteturas de aplicações

Art. 163. Deverão ser aplicados princípios de design seguro em arquiteturas de aplicações, como privilégio mínimo e validação de cada operação realizada pelo usuário, garantindo que as entradas sejam sempre verificadas, incluindo a verificação explícita de erros para dados de entrada, como tamanho, tipo e formato.

Parágrafo único. O design seguro também envolve minimizar a superfície de ataque da aplicação, como desativar portas e serviços não utilizados, remover programas desnecessários e renomear ou remover contas padrão.

Seção VIII
Do aproveitamento de módulos ou serviços controlados para componentes de segurança de aplicações

Art. 164. Deverão ser aproveitados módulos ou serviços controlados para componentes de segurança, incluindo gestão de identidade, criptografia e auditoria de **logs**. Esses recursos devem reduzir a carga de trabalho dos desenvolvedores e minimizar a probabilidade de erros de design ou implementação.

Seção XII
Da implementação de verificações de segurança no código

Art. 165. Deverão ser empregadas ferramentas de análise estática e dinâmica para verificar a segurança do código durante o ciclo de vida da aplicação.

Seção XIV

Da modelagem de ameaças

Art. 166. Deverá ser realizada a modelagem de ameaças para identificar e corrigir falhas de design de segurança antes que o código seja criado.

CAPÍTULO XVIII
GESTÃO DE INCIDENTES CIBERNÉTICOS

Art. 167. As diretrizes e os procedimentos relativos ao processo de gestão de incidentes cibernéticos são definidos em ato normativo do STI sobre Gestão de Incidentes Cibernéticos no Comando da Aeronáutica.

CAPÍTULO XIX
TESTES DE INTRUSÃO

Art. 168. Os procedimentos relativos ao processo de Teste de Intrusão são definidos em ato normativo do STI sobre Teste de Intrusão em Ativos da Rede de Computadores do Comando da Aeronáutica (ICA 7-62).

§ 1º O Órgão Central do STI é responsável por priorizar e manter atualizada a lista de soluções de TI que serão submetidos aos testes de intrusão.

§ 2º O CDCAER é o Elo Especializado do STI responsável por realizar os Testes de Intrusão no COMAER.

§ 3º As OM do COMAER poderão solicitar ao Órgão Central do STI a realização de Teste de Intrusão de seu interesse, conforme procedimento estabelecido na ICA 7-62.

§ 4º O escopo do teste a ser realizado estará descrito conforme previsto no Termo de Consentimento contido na ICA 7-62.

Seção I
Dos resultados dos testes de intrusão e correção das descobertas

Art. 169. Os resultados do Teste de Intrusão serão reportados à OM solicitante por meio do Relatório do Teste de Intrusão (RTI).

Art. 170. A OM solicitante deverá implementar as mitigações sugeridas no RTI, com base na política da organização e boas práticas recomendadas no relatório.

Art. 171. Quando a OM solicitante não for a OM desenvolvedora nem o Órgão Operador da Solução de TI alvo do teste, deverá coordenar as implementações das correções apontadas no RTI pelas partes envolvidas tanto no desenvolvimento quanto na hospedagem.

Parágrafo único. A OM solicitante deverá solicitar ao Elo de Coordenação do seu respectivo ODGSA a inclusão da demanda no processo de elaboração do PDTIC do COMAER, sempre que esforço necessário para realizar as correções solicitadas demandar novas contratações de TI ou atuação de Elos do

STI, com potencial de comprometer os cronogramas dos projetos do Plano Anual de Projetos do STI.

Seção II
Das medidas de segurança

Art. 172. O Elo de Coordenação do STI responsável pela OM cuja solução de TI foi alvo do teste de intrusão é responsável por informar ao Órgão Central do STI quando da conclusão da implementação das medidas de segurança.

Parágrafo único. As medidas de segurança implementadas deverão ser validadas em um novo Teste de Intrusão.

Art. 173. Quando não for possível mitigar a vulnerabilidade, o Comandante da OM solicitante deverá gerenciar o risco da não implementação das medidas de segurança em conjuntamente com seu Elo de Coordenação do STI, podendo solicitar apoio técnico ao Órgão Central do STI.

CAPÍTULO XX
DEFESA CIBERNÉTICA

Art. 174. A Defesa Cibernética é um dos processos críticos do STI e tem por finalidade proteger os ativos de informação de interesse da defesa nacional, obter dados para a produção de conhecimento de inteligência e buscar superioridade sobre os sistemas de informação de oponentes, no contexto de um planejamento nacional de nível estratégico, coordenado e integrado pelo Ministério da Defesa.

Art. 175. A Defesa Cibernética (Def Ciber) no âmbito do COMAER é de responsabilidade do STI.

Art. 176. O Órgão Central do STI deve atuar como Elo do COMAER no Sistema Militar de Defesa Cibernética (SMDC).

Art. 177. Compete ao Órgão Central do STI estabelecer níveis de alerta cibernético no COMAER até o nível laranja e propor ao EMAER o estabelecimento de níveis superiores, conforme necessário.

§ 1º Os níveis de alerta cibernético devem ser comunicados ao EMAER e ao Comando de Defesa Cibernética (ComDCiber), conforme arcabouço doutrinário do SMDC;

§ 2º O Órgão Central do STI elaborará um ato normativo que defina os critérios para a Classificação de Soluções de TI no COMAER quanto à sua criticidade.

§ 3º O Órgão Central do STI deve publicar uma TCA contendo as soluções de TI e sua classificação de criticidade aprovada pelo CDGSIPD.

Art. 178. O CDCAER é o Elo Especializado do STI na área de Defesa Cibernética.

Art. 179. As ETIR são Elos Específicos do STI nas áreas de Segurança da Informação e de Defesa Cibernética.

Art. 180. Os Elos de Coordenação do STI são os responsáveis, no âmbito de seu ODGSA, por viabilizar o cumprimento das ações de Defesa Cibernética coordenadas pelo Órgão Central do STI.

§ 1º Os Elos de Coordenação do STI devem estar integrados com o Centro de Defesa Cibernética da Aeronáutica (CDCAER) por meio de ações de coordenação que envolvam a proteção cibernética compartilhada.

§ 2º Os Elos de Coordenação do STI devem comunicar imediatamente ao Órgão Central do STI sobre todos os incidentes cibernéticos que ocorrerem no âmbito de seu ODGSA, independentemente de como tenham tomado conhecimento.

Art. 181. Os Elos de Serviço do STI devem atuar sob coordenação técnica do CTIR.FAB, ou de ETIR por ele designada, nas ações relacionadas à prevenção ou tratamento de incidentes cibernéticos.

CAPÍTULO XXI
PROCEDIMENTOS RELEVANTES

Art. 182. Os principais componentes que devem ser incluídos na criação de um documento de procedimento formal são:

I - objetivo do procedimento: detalhe o propósito específico do procedimento e como ele apoia a política existente.

II - escopo e aplicação: defina claramente a quem e a quais situações o procedimento se aplica.

III - responsabilidades: identifique os responsáveis pela execução e pelo monitoramento do procedimento.

IV - passo a passo: descreva cada etapa do processo de forma detalhada, garantindo que todas as atividades necessárias sejam cobertas.

V - recursos necessários: liste qualquer equipamento, **software**, ou outros recursos necessários para seguir o procedimento.

VI - prazos e frequência: estabeleça prazos para a conclusão de cada etapa e a frequência com que o procedimento deve ser revisitado ou atualizado.

VII - monitoramento e revisão: inclua diretrizes para o monitoramento contínuo do procedimento e os critérios para sua revisão periódica.

CAPÍTULO XXII
NÃO CONFORMIDADES

Seção I
Da política de gestão de ativos

Art. 183. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990, Decreto-lei nº 1.002, de 21 de outubro de 1969, Decreto nº 76.322, de 22 de setembro de 1975.

Art. 184. As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I - processo administrativo disciplinar de acordo com a legislação aplicável;

II - exoneração; e

III - ação judicial de acordo com as leis aplicáveis e acordos contratuais.

Art. 185. O não cumprimento das disposições estabelecidas na Política de Backup e Restauração de Dados Digitais (Anexo XIII), poderá resultar em consequências legais e/ou disciplinares para os agentes públicos ou terceiros envolvidos. As sanções aplicáveis dependerão da gravidade da infração e da reincidência no descumprimento das regras estabelecidas. As consequências podem incluir, mas não se limitam a:

I - sanções disciplinares:

a) advertência: em casos de infrações leves ou de primeira ocorrência, o agente poderá ser advertido por escrito, com registro nos seus dados funcionais.

b) suspensão: para infrações mais graves ou em caso de reincidência, o agente poderá ser suspenso, conforme estabelecido na Lei nº 8.112/1990 e demais normativas pertinentes.

c) demissão: em casos de violação grave ou de reincidência contínua, que comprometa a segurança e a continuidade das operações do COMAER, poderá ser aplicada a sanção de demissão, conforme os procedimentos legais aplicáveis.

II - sanções legais:

a) responsabilidade civil: em casos em que o não cumprimento da política resulte em danos à organização ou a terceiros, poderá haver responsabilização civil, com a obrigação de indenizar os prejuízos causados.

b) responsabilidade penal: se a infração for caracterizada como crime, os responsáveis poderão ser sujeitos às sanções previstas na legislação penal, incluindo, mas não se limitando, à Lei nº 8.112/1990, Código Penal Brasileiro e outras legislações pertinentes.

III - processo de escalonamento para repetida não conformidade:

a) primeira infração: caso a não conformidade seja identificada pela primeira vez, o responsável será notificado e orientado a corrigir a falha, podendo ser aplicada uma advertência formal;

b) segunda infração: em caso de reincidência, será instaurado um processo administrativo disciplinar para apurar as circunstâncias e aplicar as sanções cabíveis, como suspensão; e

c) reincidência contínua: se o não cumprimento se repetir, a medida disciplinar poderá ser mais rigorosa, incluindo a demissão, conforme a gravidade da infração e a análise do caso concreto.

Seção II
Da política de gestão de provedor de serviços

Art. 186. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art. 187. As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I - processo administrativo disciplinar de acordo com a legislação aplicável;

II - exoneração;

III - ação judicial de acordo com as leis aplicáveis e acordos contratuais; e

IV - rescisão contratual ao bem do serviço público.

Seção III
Da política de defesas contra malware

Art. 188. Em caso de violação desta política poderão ser aplicadas sanções previstas na Lei 8.112/1990 e outras legislações cabíveis.

Art. 189. As sanções por descumprimento podem incluir, mas não se limitam a um ou mais dos seguintes:

I - processo administrativo disciplinar de acordo com a legislação aplicável

II - exoneração; e

III - ação judicial de acordo com as leis aplicáveis e acordos contratuais.

CAPÍTULO XXIII
INSPEÇÕES DE SOLUÇÕES DE TI

Art. 190. Devem ser estabelecidos registros em mídia que permitam, posteriormente, a realização de inspeções em atividades de:

I - administração e manutenção dos ambientes operacionais dos sistemas servidores;

II - administração e manutenção de sistemas de redes locais, metropolitanas e de longa distância; e

III - desenvolvimento, operação e manutenção de sistemas aplicativos.

Art. 191. É responsabilidade dos Elos de Coordenação do STI a estruturação de equipe de inspetores, no âmbito de seus ODGSA, tomando como base o padrão estabelecido pelo framework COBIT ou outro que seja estabelecido pelo Órgão Central do STI, a fim de permitir a realização anual de Inspeção na Área da Segurança da Informação nas respectivas Organizações Militares subordinadas.

Art. 192. A Inspeção deverá ser realizada em três momentos, a saber:

I - pré-operacional – inspeção realizada antes da implantação de uma nova solução de TI, procedimento ou equipamento, analisando sua segurança e o impacto que este causará na infraestrutura;

II - periódica – inspeção realizada em intervalos de tempos pré-definidos, e com a devida autorização do Comandante, Chefe ou Diretor da OM inspecionada, devendo ser verificados, de forma minuciosa, os procedimentos de acordo com as normas de segurança da informação em vigor, com o objetivo de identificar eventuais falhas e corrigi-las antes de causarem qualquer tipo de prejuízo; e

III - emergencial – sempre que houver uma falha de segurança, esta inspeção deve ser realizada para evidenciar as causas da vulnerabilidade e buscar formas de corrigir o problema.

Art. 193. Os inspetores serão pessoas estranhas ao local no qual será realizada a inspeção, de forma a evitar vícios e comprometimentos que possam afetar o processo de inspeção.

Art. 194. As Organizações Militares deverão sofrer processos de inspeção com uma periodicidade mínima de 02 (dois) anos.

Art. 195. O Relatório de Inspeção de Sistemas deverá ser elaborado em duas vias, onde deverão ser apontadas todas as incorreções e irregularidades observadas pela equipe de inspetores.

Art. 196. Uma via do Relatório de Inspeção de Sistemas deverá ser encaminhada para a OM inspecionada para resposta no prazo de 30 (trinta) dias.

Art. 197. Uma via do Relatório de Inspeção de Sistemas deverá ser encaminhada ao Órgão Central do STI e mantida por 10 (dez) anos para eventuais consultas.

CAPÍTULO XXIV
PLANO DE CONTINUIDADE DE NEGÓCIOS EM SEGURANÇA DA INFORMAÇÃO

Art. 198. Cada um dos sistemas de TI considerados críticos pelo COMAER deve estar protegido por um Plano de Continuidade de Negócios em Segurança da Informação. A competência para a elaboração e a implantação desse Plano pertence ao gestor do sistema, seja Elo de Coordenação ou Elo Especializado do STI.

Art. 199. Os serviços de TI críticos do COMAER serão elencados por cada ODGSA e compilados pelo Órgão Central do STI, sendo submetidos à apreciação do Comitê de Governança Digital, de Segurança da Informação e de Proteção de Dados (CGDSIPD) para ratificação ou retificação.

Art. 200. Os critérios mínimos utilizados para a confecção de Planos de Continuidade de Negócio em Segurança da Informação serão definidos em legislação complementar emitida pelo Órgão Central do STI, e os critérios complementares emitidos em legislação pelo respectivo Órgão de Direção Setorial do COMAER (ODGSA).

CAPÍTULO XXV
OUTRAS SOLUÇÕES DE TI

Seção I
Do emprego de VoIP

Art. 201. Os projetos que visam o emprego de VoIP como solução técnica para atender necessidades de Organizações do COMAER deverão ser submetidos ao DECEA para análise e aprovação, com antecedência mínima de 90 (noventa) dias de sua data prevista de entrada em operação.

Art. 202. Os critérios utilizados para emissão de autorização para uso de VoIP serão estabelecidos em instrução específica emitida pelo Órgão Central de Telecomunicações (DECEA).

Seção II
Do emprego de videoconferência

Art. 203. Os projetos que visam à implantação de soluções de videoconferência para atender a necessidades de Organizações do COMAER deverão ser submetidos à DTI, Órgão Central do STI, para análise e aprovação, com antecedência mínima de 90 (noventa) dias de sua data prevista de entrada em operação.

Art. 204. Os critérios utilizados para emissão de autorização para uso de videoconferência serão estabelecidos em instrução específica emitida pela DTI, Órgão Central do STI.

Art. 205. Está autorizado o uso de serviços de videoconferência ou VoIP de âmbito interno da Organização (rede local) ou entre Organizações (Intraer), desde que seja informado ao Órgão Central do STI a solução utilizada.

Art. 206. Está autorizado o uso de serviços de videoconferência ou VoIP via Internet, para assuntos exclusivos da OM, desde que se utilize uma solução com criptografia comercial e que não sejam tratados assuntos sigilosos.

Art. 207. O sistema de videoconferência de âmbito interno da Organização (rede local) e entre Organizações (Intraer) de qualquer teor de assunto e as videoconferências onde serão tratados assuntos sigilosos deverão ser os padronizados e mantidos pela DTI.

Art. 208. O uso de redes sociais para assuntos institucionais exclusivos da OM pode ser implantado, desde que se utilize ponto de acesso à Internet não conectado à Intraer e que não sejam tratados assuntos sigilosos.

Seção III
Da computação em nuvem

Art. 209. A implementação de soluções e serviços com hospedagem em nuvem devem seguir as regras previstas na Norma NBR ABNT ISO/IEC 27017 e da IN GSI Nº 5/2021, desde que não sejam hospedados dados e informações sigilosas.

Art. 210. A utilização de quaisquer serviços hospedados em nuvem por alguma Organização Militar do COMAER requererá autorização prévia do respectivo ODGSA, após cuidadosa análise de riscos.

Parágrafo único. Os ODGSA poderão solicitar assessoramento técnico do STI mediante solicitação formaal ao Órgão Central do STI.

CAPÍTULO XXVI
COLABORADORES TERCEIRIZADOS

Art. 211. Os dispositivos legais utilizados para a contratação de colaboradores terceirizados devem contemplar cláusulas que estabeleçam controles de segurança para os sistemas de TI envolvidos, principalmente as relativas ao estabelecimento de termo de confidencialidade entre as contratadas, conforme normativas estabelecidas na ICA 200-4/2007 (Processo de Concessão de Credencial de Segurança de Pessoa Jurídica).

Art. 212. Todos os contratos em vigor, que envolvam direta ou indiretamente acesso a dados sigilosos, também deverão ser revisados pelo CIAER a fim de assegurar que recursos críticos não estejam sendo acessados por pessoal terceirizado não credenciado.

Art. 213. Os colaboradores terceirizados devem ser geridos conforme a Política de Gestão de Provedor de Serviços (Anexo XXIII).

CAPÍTULO XXVII
TRATAMENTO DE DADOS PESSOAIS

Art. 214. As diretrizes para o tratamento de dados pessoais no âmbito do COMAER constam na DCA 16-6/2022 – Governança da Proteção de Dados Pessoais do Comando da Aeronáutica, que ensejaram a criação da Política de Proteção De Dados Pessoais desta NSCA (Anexo XXIV), cujo cumprimento é obrigatório no âmbito do COMAER.

CAPÍTULO XXVIII
DISPOSIÇÕES TRANSITÓRIAS

Art. 215. O Órgão Central do STI elaborará um Plano de Adequação do Comando da Aeronáutica ao Programa de Privacidade e Segurança da Informação do Governo Federal.

§ 1º Este plano deverá ser encaminhado ao EMAER pelo Órgão Central do STI em até 180 dias da publicação desta NSCA.

§ 2º Compete ao CGDSIPD a aprovação do Plano de Adequação do Comando da Aeronáutica ao Programa de Privacidade e Segurança da Informação do Governo Federal.

CAPÍTULO XXIX
DISPOSIÇÕES FINAIS

Art. 216. Todos os usuários de recursos computacionais do COMAER devem assinar o Termo de Ciência e Compromisso com as Políticas de Segurança da Informação (Anexo XIX).

Parágrafo único. Os Elos do STI devem condicionar a utilização de recursos computacionais do COMAER, em seu escopo de atuação, à assinatura desse Termo.

Art. 217. Todo o efetivo do COMAER, bem como provedores de serviços ao COMAER, são responsáveis por aderir às práticas de segurança da informação estabelecidas e relatar qualquer atividade suspeita o mais rápido possível.

Art. 218. Compete ao Órgão Central do STI buscar o apoio contínuo da alta administração para a implementação e execução eficaz desta NSCA e de suas políticas, alocando recursos adequados e priorizando a segurança cibernética como uma preocupação organizacional.

Art. 219. O Órgão Central do STI coordenará periodicamente a avaliação do impacto desta NSCA e das suas Políticas na segurança geral do COMAER, identificando áreas de sucesso e oportunidades de melhoria.

Art. 220. Os integrantes do CGDSIPD poderão expedir instruções complementares, no âmbito de suas competências, que detalharão suas particularidades e procedimentos das Políticas, alinhadas às diretrizes emanadas pelo CGDSIPD e ao PEMAER.

Art. 221. As dúvidas sobre esta NSCA e seus anexos serão submetidas ao Órgão Central do STI.

Art. 222. Esta NSCA e suas políticas devem ser comunicadas para partes externas, como fornecedores e parceiros, para promover a conscientização e colaboração na proteção contra ameaças.

Art. 223. Os casos não previstos nesta Norma serão submetidos à apreciação do Diretor de Tecnologia da Informação da Aeronáutica, que consultará o CGDSIPD sempre que o assunto extrapolar suas competências legais.

Art. 224. Esta NSCA e suas políticas deverão ser revisadas anualmente ou sempre que houver mudanças significativas nas legislações que a regem.

ANEXO II
POLÍTICA DE USO DE RECURSOS COMPUTACIONAIS

Art. 1º Esta Política aplica-se a todos os usuários, internos e externos, que utilizam os recursos computacionais do COMAER, incluindo servidores, computadores, redes, sistemas de informação e dispositivos móveis. O cumprimento desta política é obrigatório e qualquer violação poderá resultar em sanções disciplinares.

Seção I
Dos recursos computacionais

Art. 2º Os recursos computacionais do COMAER têm por finalidade servir à pesquisa, ao desenvolvimento, ao ensino e às atividades técnicas, administrativas e operacionais de interesse do serviço.

Art. 3º O uso dos recursos computacionais do COMAER está sujeito às leis federais.

Art. 4º Quanto ao uso da Internet no COMAER, os usuários devem observar, além dos normativos internos, as normas e recomendações do Comitê Gestor da Internet no Brasil (CGI.BR).

Seção II
Da autorização de uso

Art. 5º O usuário, para utilizar os recursos computacionais do COMAER, deve solicitar ao Elo de Serviço de sua OM a abertura de uma conta de usuário, a qual o identificará univocamente.

Seção III
Das contas de usuários

Art. 6º A solicitação de abertura de Contas de usuário, tanto em recursos computacionais locais como em corporativos, se dá pelo preenchimento da Ficha de Cadastro de usuário, conforme estabelecido por cada OM do COMAER. A ficha deve ser assinada pelo solicitante e pelo responsável da seção onde o usuário está desempenhando suas atividades.

Art. 7º O responsável pela solicitação da Conta de usuário deve providenciar a abertura junto à equipe de TI da OM.

Art. 8º A OM poderá definir procedimentos adicionais para a abertura de Contas de usuário em recursos computacionais locais.

Subseção I
Do uso das contas de usuários

Art. 9º A Conta de usuário e a respectiva senha são atribuídas a um único usuário e são intransferíveis. O usuário assume integral responsabilidade pela guarda e sigilo da senha, bem como pelo uso indevido por terceiros.

Art. 10. As senhas devem ser tratadas como informação classificada do COMAER.

Art. 11. O usuário é individualmente responsável por todas as atividades realizadas com sua Conta de usuário nos recursos computacionais do COMAER.

Art. 12. As senhas utilizadas pelos usuários devem atender, no mínimo, aos seguintes requisitos:

I - complexidade adequada (incluindo letras maiúsculas e minúsculas, números e caracteres especiais);

II - troca periódica de senha;

III - O comprimento mínimo de 8 caracteres para senhas com autenticação por múltiplos fatores (MFA) e 14 caracteres para senhas sem MFA;

IV - não devem conter nomes, sobrenomes, números de documentos, placas de carros, números de telefones e datas;

V - não devem conter palavras que façam parte de dicionários, ou seja, nomes de músicas, filmes e outros;

VI - priorizar a utilização de frases complexas no lugar de palavras ou a utilização de maiúsculas e minúsculas, números, sinais de pontuação e símbolos; e

VII - não devem fazer parte de bases públicas de senhas previamente comprometidas.

Art. 13. As contas de usuário e senhas não devem ser inseridas em mensagens de e-mail ou qualquer outra forma de comunicação eletrônica, escritas em papel, bilhetes colados nos Recursos Computacionais ou guardadas em qualquer local.

Art. 14. Não deve ser usada senha única para Contas de usuários diferentes e para sistemas autônomos diferentes.

Art. 15. Todas as senhas de usuário, após o primeiro acesso aos recursos computacionais, devem ser imediatamente trocadas.

Art. 16. Todas as senhas existentes em recursos computacionais recebidos de terceiros devem ser substituídas.

Art. 17. Senhas suspeitas de terem sido descobertas deverão ser imediatamente

trocadas.

Art. 18. O acesso a um recurso computacional, após 3 (três) tentativas com erros de Conta de usuários e/ou senha, deverá ser bloqueada. A reativação da Conta de usuário deverá ser solicitada à equipe de TI da OM.

Seção IV
Do uso dos recursos computacionais

Art. 19. O usuário é responsável pelos eventuais arquivos e informações de cunho pessoal que possam existir nos recursos computacionais do COMAER, sendo que os mesmos, para todos os efeitos, não estão sujeitos a qualquer regime de privacidade e são passíveis de monitoramento e inspeção pelo CTIR.FAB ou pela Equipe de Segurança em TI da respectiva OM, em consonância com as normas e legislação vigente.

Art. 20. O usuário é responsável pelo uso da informação a que tiver acesso, bem como pela sua distribuição.

Art. 21. Toda informação armazenada nos recursos computacionais ou transmitida, pela Rede Local ou pela Intraer, será tratada e considerada pertencente à respectiva OM.

Art. 22. O usuário é responsável pelo **backup** e recuperação das informações existentes em sua estação de trabalho e pelo armazenamento das correspondentes mídias.

Art. 23. Quando utilizar recursos computacionais portáveis do COMAER, o usuário deverá realizar cópia de segurança, não conectá-los em redes externas não pertencentes ao COMAER (ou se necessário, prover os cuidados adequados), não permitir seu uso por terceiros (exceto sob consentimento explícito do responsável), provê-los de mecanismo de trava física e lógica e, em hipótese alguma, deixá-los desprotegidos em áreas públicas, devolvendo-os ao setor responsável após o seu uso.

Art. 24. O usuário deve comunicar, imediatamente, ao seu chefe imediato e ao responsável direto pelo recurso computacional do local onde o fato tenha ocorrido, qualquer violação das regras contidas neste Anexo ou prejuízos causados por terceiros, a eles próprios e aos recursos computacionais do COMAER.

Art. 25. Os Administradores de Segurança de TI das OM, ou, na sua ausência os Administradores de Rede das OM, preferencialmente, deverão possuir telefones celulares funcionais cujo número deverá ser divulgado para acionamento a qualquer tempo.

Art. 26. Qualquer mau funcionamento de um sistema deverá ser imediatamente reportado à equipe de TI da OM, pois a demora neste ato poderá levar a sérios danos aos sistemas, e até mesmo à indisponibilidade dos Recursos Computacionais envolvidos.

Art. 27. Informações a respeito de medidas de segurança são confidenciais e não devem ser reveladas para pessoas não autorizadas.

Art. 28. Os Recursos Computacionais somente poderão se conectar fisicamente às redes de dados do COMAER.

Art. 29. Todas as mídias removíveis, independentes da fonte, devem ser verificadas com programa antivírus antes de serem utilizadas.

Art. 30. Os usuários são responsáveis por eventuais disseminações de vírus em seus sistemas sempre que não observarem as medidas previstas na Política de Antivírus e Códigos Maliciosos (Anexo V), devendo notificar imediatamente à equipe de TI da OM, caso ocorra algum incidente.

Art. 31. O usuário deve observar o estabelecido na política para recebimento (**download**) de arquivos, por e-mail ou qualquer outro meio eletrônico, conforme consta na Política de Antivírus e Códigos Maliciosos (Anexo V).

Art. 32. É vedado ao usuário a realização das seguintes ações:

I - utilizar os recursos computacionais para fins diversos dos funcionais ou institucionais, em desacordo com este Anexo e com as demais publicações vigentes no COMAER;

II - efetuar acesso não autorizado, atacar ou monitorar os recursos computacionais ou redes de dados, utilizando recurso da rede local da OM ou outros meios;

III - tentar ou efetuar acesso não autorizado a arquivos confidenciais do COMAER;

IV - próprio acesso, por meio do monitoramento do barramento de dados, ou das redes de dados existentes no COMAER;

V - tentar ou efetuar a interferência em serviços de outros usuários ou o seu bloqueio, utilizando recursos da rede local da OM ou outros meios;

VI - violar ou tentar violar os sistemas de segurança dos recursos computacionais do COMAER, como quebrar ou tentar adivinhar contas de usuário ou senha de terceiros;

VII - utilizar **softwares** em desacordo com este Anexo;

VIII - instalar ou manter programas maléficos dentro da rede ou de servidores, como vírus, **worms**, cavalos-de-tróia, **adware**, **spyware**, **mail bombs**, **backdoor**, **keylogger**, **bots**, **botnets**, e assemelhados que possam colocar em risco os recursos computacionais;

IX - utilizar serviços de redes sociais, mensagens instantâneas ou de bate-papo disponíveis na Internet (aqueles hospedados e mantidos por entidade externa ao COMAER) sem autorização expressa do Órgão Central do STI;

X - interromper processos de rastreamento de vírus;

XI - utilizar, armazenar ou distribuir, nas redes de comunicação e nos recursos computacionais do COMAER, informações indesejadas, tais como, correntes de cartas, circulares e similares, materiais obscenos, ofensivos, ilegais, não éticos, comercial privado, propagandas, ameaças, difamação, injúria, racismo, spam ou outro que venham a causar molestamento, tormento ou danos a terceiros;

XII - utilizar, armazenar ou distribuir material com conteúdo que incentive ou instrua a invasão de recursos computacionais ou redes de computadores;

XIII - instalar, alterar, configurar ou excluir os recursos computacionais, tanto de **hardware** como de **software**, existentes tanto nas redes locais como na Intraer;

XIV - remanejar recursos computacionais sem a prévia autorização do responsável por seu Setor Funcional e sem o prévio conhecimento da equipe de TI da OM;

XV - acessar simultaneamente um mesmo recurso computacional. Caso o usuário identifique um acesso simultâneo deverá imediatamente comunicar à equipe de TI da OM, sob pena de responder por sua omissão;

XVI - fazer má utilização dos recursos computacionais, expondo-os a choques elétricos ou magnéticos, líquidos e outros fatores que possam provocar danos aos mesmos;

XVII - realizar a transferência de qualquer informação ou documento classificado, existente nos recursos computacionais do COMAER, sem a prévia autorização do Responsável por seu Setor Funcional, sem a devida proteção criptográfica e sem a utilização da Rede de Comunicação de Dados Sigilosos (Rede Mercúrio), mantida e normatizada pelo CIAER;

XVIII - utilizar processo criptográfico em arquivos contendo informação ou documentos, mesmo que de caráter pessoal, residentes nos recursos computacionais de propriedade do COMAER, sem que para isso tenha autorização;

XIX - utilizar processo criptográfico em arquivos contendo informação ou documento não ostensivos residentes nos recursos computacionais, diferente do padrão definido, sem conhecimento do

Chefe da equipe de TI da OM ou de quem por ele tenha sido investido nesse poder;

XX - impedir ou dificultar, de alguma forma, a realização das atividades de monitoramento e inspeção dos recursos computacionais do COMAER; e

XXI - realizar qualquer outro procedimento de uso dos recursos computacionais não previsto neste Anexo, que possa afetar de forma negativa o COMAER, outras organizações e seus usuários.

Seção V
Do uso de Software

Art. 33. O usuário deve respeitar os direitos de propriedade intelectual, em particular os que se referem à lei em vigor que dispõe sobre a proteção da propriedade intelectual de programa de computador e sua comercialização no País.

Art. 34. O usuário deve observar que toda e qualquer utilização dos recursos computacionais do COMAER deverá estar de acordo com todas as obrigações contratuais assumidas pelo COMAER, inclusive no que respeita às limitações definidas nos contratos de **software** e outras licenças.

Art. 35. Os **softwares** cedidos por produtores ou seus representantes legais, a título de demonstração ou teste, deverão estar acompanhados de contratos específicos formalizados.

Art. 36. O **software** de propriedade do usuário ou por ele contratado de terceiros, deverá estar acompanhado do seu contrato específico formalizado ou seu Termo de Responsabilidade, juntamente com o comprovante de registro do produto, quando da utilização do mesmo no âmbito do COMAER e sua utilização só poderá ser realizada com a autorização da equipe de TI da OM.

Art. 37. Os **softwares** classificados como de domínio público (**freeware**) seguirão orientação específica de cada Elo de Serviço, desde que o **software** seja gratuito para uso corporativo.

Art. 38. É vedado ao usuário de qualquer **software**:

I - escrever, gerar, compilar, copiar, propagar, executar ou tentar introduzir nos recursos computacionais do COMAER, códigos ou **software** contendo processos destrutivos;

II - invadir recursos computacionais do COMAER, com exceção daqueles usuários cuja função esteja relacionada com a utilização destas ferramentas para os fins de monitoramento e inspeção;

III - utilizar os **softwares** do COMAER em atividades particulares;

IV - explorar, sem autorização, aplicações e sistemas corporativos para obter dados ou alterar dados; e

V - possuir senha de administrador de estação de trabalho, a fim de que não efetue instalação de **software**.

ANEXO III
POLÍTICA DE ADMINISTRAÇÃO DE RECURSOS COMPUTACIONAIS

Art. 1º Na administração dos recursos computacionais do COMAER, os Elos do STI devem observar as regras da Política contida neste Anexo e aplicá-las no âmbito de seu escopo de atuação.

Seção VI
Da administração de Recursos Computacionais

Art. 2º O Órgão Central do STI deve definir e os Elos do STI devem implementar e manter um único Sistema de Cadastro de Contas de usuários contendo informações cadastrais de todas as contas existentes em cada OM ne seu escopo de atuação, seja em recursos computacionais corporativos, seja em recursos computacionais locais.

Art. 3º Os Elos do STI devem, também:

I - priorizar, quando possível, a integração com o Servidor de Autenticação de Login Único do STI;

II - abrir, gerenciar e encerrar contas de usuários;

III - garantir que durante a abertura de conta o usuário assine um Termo de Compromisso e Manutenção de Sigilo, declarando ler e cumprir a presente norma, além de cumprir as leis de direitos autorais e as legislações de proteção de dados;

IV - prover uma única conta para cada usuário, mantendo-a igual em todos os recursos computacionais locais nos quais ele vier a ter acesso, quando viável tecnologicamente; e

V - validar anualmente as contas de usuários na sua rede local, por meio de um inventário de contas.

Art. 4º O inventário de contas deve registrar as seguintes informações para cada conta:

I - nome completo da pessoa;

II - nome de usuário;

III - datas de início e término de validade da conta;

IV - setor associado para contas de usuário; e

V - setor proprietário, data de revisão e propósito para contas de serviço.

Art. 5º A validação periódica do inventário de contas deve ocorrer, no mínimo, a cada três meses, garantindo que todas as contas ativas estejam devidamente autorizadas e atualizadas.

Art. 6º O inventário de contas deve incluir, no mínimo, as seguintes informações para cada conta:

I - tipo de conta (serviço, administrador, usuário);

II - nome do usuário;

III - datas de início e término de validade da conta; e

IV - seção associada à conta.

Art. 7º Para centralizar a gestão de contas por meio de um serviço de diretório ou identidade, devem ser observados os seguintes requisitos mínimos:

I - selecionar e implementar um serviço de diretório ou identidade adequado, como **Active Directory** (AD), **Azure Active Directory** (Azure AD), ou LDAP (**Lightweight Directory Access Protocol**), conforme as necessidades da organização;

II - configurar e integrar o serviço de diretório a todos os sistemas e aplicações que exijam gestão de contas;

III - implementar automação para criação, atualização e exclusão de contas, visando a redução de erros e maior eficiência;

IV - gerenciar os ciclos de vida das contas, desativando ou excluindo contas inativas após 45 dias, quando possível; e

V - aplicar controles de segurança adequados para proteger as informações do diretório contra acessos não autorizados e realizar validações periódicas para garantir a conformidade com as políticas de segurança vigentes.

Art. 8º Consultar, periodicamente, os Chefes dos Setores Funcionais quanto às atualizações das informações cadastrais pertinentes aos seus usuários.

Art. 9º Manter mecanismos para exigir dos usuários a mudança de senha sempre que evidências de comprometimento forem identificadas ou em intervalos de até 360 (trezentos e sessenta) dias.

Art. 10. Manter mecanismos para impedir a repetição de senhas considerando as seis últimas senhas utilizadas.

Art. 11. Prover meios para moderar a utilização de mensagens instantâneas ou de bate-papo disponíveis na Internet que sejam hospedados e mantidos por entidades externas ao COMAER e não autorizados pelo Órgão Central do STI.

Art. 12. Prover mecanismos para bloquear a conta de usuário após 3 (três) tentativas de acesso a um recurso computacional com erros de conta de usuário e/ou senha.

Art. 13. Prover meios para suspender, encerrar as sessões e ativar protetores de tela padronizados institucionalmente, após um período de inatividade de, no máximo:

I - 15 minutos, para dispositivos de uso geral;

II - 2 minutos, para dispositivos móveis; e

III - 1 minuto, para dispositivos que tratem dados sensíveis.

Parágrafo único. Os protetores de tela devem ser desativados automaticamente com o uso da senha.

Art. 14. Prover a segurança e a integridade dos recursos computacionais disponíveis, dos serviços aos usuários e dos dados armazenados nas máquinas servidoras sob sua responsabilidade, atentando para os requisitos previstos nas normas vigentes de Proteção de Dados.

Art. 15. Agendar e realizar o processo de execução de cópias de segurança (**backup**) de Servidores e armazenar as mídias correspondentes conforme procedimento definido nesta Norma.

Art. 16. Manter os recursos computacionais sempre atualizados, pesquisando, obtendo e aplicando, sempre que possível, os pacotes de correção e atualização disponibilizados pelos fabricantes, atentando também para os pacotes de terceiros que sejam dependências dos recursos computacionais utilizados nas redes locais.

Art. 17. Suspender temporariamente o acesso de qualquer usuário a todo e qualquer recurso computacional sob sua responsabilidade, nos casos de suspeita de violação desses recursos computacionais. Se comprovada a violação dos recursos, pelo usuário, deverá ser encaminhada pela Chefia da equipe de TI da OM, Parte Administrativa ao Comandante, Chefe ou Diretor da OM, para que sejam tomadas as medidas cabíveis, determinando a abertura de sindicância ou mesmo inquérito, sob pena de que a Chefia da equipe de TI ou mesmo o Comandante da Unidade responderem solidariamente pelos danos causados. Nos casos em que forem comprovados danos ao erário, o processo deverá ser encaminhado à SEFA para providências.

Art. 18. Isolar da rede local os recursos computacionais com suspeita de violação e seguir os procedimentos propostos pelo CDCAER.

Art. 19. Suspender temporariamente serviços de rede local em caso de violação ou suspeita de violação dos recursos computacionais locais, informando o fato ao Comando/Chefia/Direção da OM.

Art. 20. Difundir constantemente as normas e procedimentos para uso de recursos computacionais, estabelecidos na Política de Uso de Recursos Computacionais (Anexo II).

Art. 21. Analisar a rede local sob a sua responsabilidade, utilizando **software** ou equipamento apropriado, com o objetivo de garantir um desempenho adequado sem, no entanto, afetar ou alterar qualquer configuração de outra rede local, que não esteja sob a sua responsabilidade.

Art. 22. Configurar servidores de e-mail para gerar automaticamente estatísticas de uso de cada usuário, sempre que possível.

Art. 23. Realizar alterações de emergência na rede de comunicação de dados para prevenir mudanças inadvertidas que podem levar à negação de serviços, revelação de informação não autorizada e outros problemas análogos.

Art. 24. Realizar monitoramento e inspeção na utilização dos recursos computacionais locais, quando autorizado pelo Comando, Chefia e/ou Direção da respectiva OM, visando preservar a integridade das informações institucionais e a imagem do COMAER, podendo fiscalizar:

I - conteúdo de mensagens transmitidas e recebidas;

II - arquivos residentes em discos;

III - programas de computadores instalados;

IV - fluxo de pacotes na rede local;

V - arquivos específicos de controle;

VI - programas de computador em execução; e

VII - outros recursos computacionais.

Art. 25. Limitar a área reservada aos usuários no servidor de e-mail e estabelecer um prazo máximo para a manutenção de mensagens não superior a 180 (cento e oitenta) dias, dando ciência destes fatos aos usuários. Ao término deste prazo, as mensagens deverão ser retiradas do sistema e tratadas conforme critério da OM.

Art. 26. Envidar esforços para evitar o acesso simultâneo de mais de um usuário a um mesmo recurso computacional, evitando assim possíveis acessos não autorizados.

Art. 27. Impedir, durante o registro de senhas, a utilização de senhas comuns, fracas ou comprometidas. Comparar a senha escolhida com bases públicas de senhas previamente comprometidas, palavras de dicionários, caracteres repetidos, entre outros.

Art. 28. Informar ao usuário a política de senhas em uso.

Art. 29. Responsabilizar-se por outras tarefas inerentes à sua função que forem determinadas pelo Comando/Chefia/Direção.

Art. 30. Conceder privilégios de sistema para atender o mínimo necessário à realização das atividades dos usuários, reavaliando-os periodicamente para que os privilégios desnecessários sejam revogados.

Art. 31. Instalar em todos os recursos computacionais utilizados pelos usuários um **software** antivírus homologado e atualizado, de preferência corporativo, conforme estabelecido na Política de Antivírus e Códigos Maliciosos (Anexo V).

Art. 32. Desabilitar a opção de execução automática de arquivos anexados dos **softwares** clientes de correio eletrônico.

Art. 33. Garantir que todos os ativos institucionais utilizem protocolos seguros, como SSH e HTTPS, para gerenciamento remoto, sendo vedado o uso de protocolos inseguros, exceto em casos operacionais estritamente essenciais e devidamente justificados, incluindo, mas não se limitando a:

I - Telnet;

II - HTTP;

III - FTP (**File Transfer Protocol**); e

IV - RDP (**Remote Desktop Protocol**) sem criptografia.

Art. 34. Modems e quaisquer outros dispositivos de conexão remota à rede deverão ser desinstalados ou desabilitados nos Recursos Computacionais.

Art. 35. Zelar para que os sistemas multiusuários ou sistemas de dados incluam ferramentas automatizadas para verificação do estado de segurança dos sistemas. Estas ferramentas devem incluir meios para registro, detecção e correção de problemas de segurança.

Art. 36. Zelar para que os desenvolvedores de aplicativos garantam que seus programas suportam a autenticação de usuários individuais, e não de grupos.

Art. 37. Dar ciência aos usuários que todas as atividades relacionadas ao uso dos recursos computacionais do COMAER são passíveis de registro, monitoramento e inspeção, em compatibilidade com as normas vigentes de Proteção de Dados.

Art. 38. Ajustar o tamanho máximo permitido para envio e/ou de mensagens e/ou arquivos segundo necessidades de sua OM.

Art. 39. Desativar caixas postais não acessadas por um período de mais de 60 (sessenta) dias, desde que não justificado.

Art. 40. Configurar o **software** de **e-mail** para pedir senha ao entrar na conta de correio.

Art. 41. Controlar a utilização de ferramentas de navegação e extensões de navegador conforme os critérios abaixo:

I - avaliação de necessidade:

a) apenas ferramentas e extensões essenciais para as atividades profissionais devem ser permitidas nos navegadores web dos ativos corporativos; e

b) o responsável por cada departamento deve justificar a necessidade operacional de ferramentas solicitadas.

II - lista de ferramentas autorizadas:

a) o Órgão Central do STI deve manter uma lista de ferramentas e extensões de navegador aprovadas, revisando-a periodicamente; e

b) qualquer instalação fora dessa lista será considerada uma violação das políticas de segurança e poderá ensejar em medidas disciplinares.

III - controle de instalação:

a) permissões de instalação devem ser controladas centralmente pela equipe de TI. Usuários finais não devem ter permissões para instalar ou habilitar extensões sem aprovação prévia; e

b) ferramentas de monitoramento devem ser implementadas para detectar e bloquear automaticamente a instalação de extensões ou **softwares** não autorizados.

IV - desinstalação de ferramentas não autorizadas:

a) ferramentas não autorizadas devem ser removidas imediatamente pelos administradores de sistema e os usuários envolvidos devem ser notificados sobre a violação; e

b) caso ferramentas não autorizadas sejam detectadas repetidamente em um dispositivo, um plano de ação corretiva deve ser executado, incluindo a revisão de privilégios de instalação e o reforço da política.

ANEXO IV
POLÍTICA DE MANIPULAÇÃO DE INFORMAÇÕES CLASSIFICADAS

Art. 1º Para o armazenamento e tramitação seguros de informações classificadas (sensíveis), deve-se observar o disposto a seguir:

I - dados e informações classificadas deverão ser transmitidos por meio eletrônico, desde que obrigatoriamente criptografado, em sistema de cifra de alta confiabilidade, com algoritmo de Estado, homologado pelo CIAER conforme preconizado a Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica;

II - os acessos às informações classificadas devem ser registrados e exigir a autenticação do usuário, do Recurso Computacional e do ponto de acesso;

III - sendo possível, o sistema deverá emitir avisos para o Administrador de Rede Local no caso de tentativas de acessos não autorizados aos dados classificados;

IV - a transmissão de dados classificados somente poderá ocorrer com a utilização de um mecanismo de criptografia, utilizando-se de um programa de encriptação de dados, observando-se o disposto na RCA 205-1;

V - dados classificados e mantidos nos Recursos Computacionais do COMAER deverão estar criptografados observando o disposto no RCA 205-1;

VI - as cópias de segurança (**backup**) devem ser mantidas de acordo com a Política de Segurança Lógica (Anexo XI) e com a Política de Backup e Restauração de Dados Digitais (Anexo XIII).

VII - informações classificadas devem ser tratadas conforme preconizado na ICA 205-47/2015 – Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica;

VIII - toda exclusão de informações classificadas deverá ser executada através de um processo de apagamento seguro;

IX - quando os recursos computacionais não estiverem sendo utilizados e as informações neles contidas forem classificadas, estas deverão ser apagadas. Caso seja necessário que estas informações permaneçam no recurso computacional, o mesmo deverá ser armazenado em local seguro, com acesso restrito ao pessoal responsável;

X - em caso de extravio de recursos computacionais contendo informações classificadas, o Setor de Inteligência da OM deverá ser imediatamente comunicado pelo Comando/Chefia/Direção da OM via parte reservada, e todas as chaves compartilhadas em outros recursos deverão ser trocadas;

XI - deverá ser aberto, a critério do Comandante, Chefe ou Diretor da OM, processo de sindicância para apuração do extravio de recursos computacionais;

XII - deverá ser aberto Boletim de Ocorrência na Delegacia mais próxima da ocorrência do extravio caso o mesmo tenha ocorrido externamente às dependências da OM;

XIII - deve existir uma ferramenta para verificação regular e automática da integridade e autenticidade dos dados classificados em uso para alertar os administradores de rede sobre toda e qualquer alteração;

XIV - sempre que a encriptação for usada, a versão original do documento deverá ser

apagada após a execução do processo de decriptação e verificado o correto restabelecimento da versão original;

XV - chaves de encriptação usadas pelo COMAER são sempre tratadas como informações classificadas e, portanto, não podem ser reveladas para consultores, trabalhadores temporários ou similares. O acesso a estas chaves devem ser restrito ao pessoal autorizado e a quem tem a necessidade de usá-las;

XVI - não deverá ser feita a impressão de informações classificadas em dispositivos de impressão de rede.

XVII - até onde o sistema operacional permitir, o manuseio de informações classificadas ou críticas deve ser registrado quanto a quaisquer eventos relacionados à segurança; e

XVIII - elaborar o Relatório de Impacto de Proteção de Dados (RIPD) nos processos, projetos e serviços que utilizarem informações classificadas contendo dados pessoais para fins de Defesa Nacional, segurança do Estado, que poderão ou deverão ser solicitados pela Autoridade Nacional de Proteção de Dados (ANPD) nos casos previstos na Lei Geral de Proteção de Dados Pessoais (LGPD).

ANEXO V
POLÍTICA DE ANTIVÍRUS E CÓDIGOS MALICIOSOS

Art. 1º Com relação a esta Política, são definidos os requisitos abaixo relacionados à prevenção, detecção e erradicação de vírus, contaminações e códigos maliciosos nos recursos computacionais:

I - todos os computadores do COMAER devem ter instalado um programa antivírus, fornecido ou recomendado pelo Órgão Central do STI, devidamente licenciado e atualizado;

II - preferencialmente, o servidor que executa o antivírus corporativo na OM deve

III - ser dedicado;

IV - os computadores infectados devem ser fisicamente desconectados da rede até que seja garantida a sua descontaminação;

V - o programa antivírus deve ser configurado para que seja periodicamente atualizado e executado em intervalos regulares, de preferência de maneira automática;

VI - o **software** antivírus emitirá alerta quando ocorrer a detecção de **malware**. O CTIR.FAB deve possuir acesso ao servidor principal do antivírus corporativo, de modo a ter acesso às informações de detecção de **malware**;

VII - sempre que possível, habilitar no recurso computacional a opção de verificação automática de vírus nas mídias removíveis;

VIII - os recursos computacionais, sempre que possível, deverão estar protegidos contra códigos maliciosos do tipo **adware**, **spyware**, cavalo-de-tróia (**trojans**), **worms**, **backdoors**, **keyloggers**, **bots**, **botnets**, **rootkit** e outros que possam surgir; e

IX - fica estabelecida a seguinte política para download (recebimento) de arquivos, por e-mail ou qualquer outro meio eletrônico:

a) excepcionalmente, e quando estritamente necessário ao exercício das atividades funcionais do usuário, será permitido o recebimento de arquivos comerciais, tais como imagens, textos e outros, que deverão ser rastreadas (“escaneados”) por antivírus antes de serem abertos;

b) é estritamente proibido o carregamento de qualquer arquivo executável recebido pelos usuários, colaboradores ou prestadores de serviços com extensões do tipo EXE, .COM,.SCR, ou outros que possam comprometer o sistema através da execução de comandos maliciosos, vírus, trojans e outros similares; e

c) quando se tratar de atualização de **software**, que envolva arquivos deste tipo, a equipe de TI da OM será a responsável por executar o serviço.

X - o CDCAER poderá assessorar o Órgão Central do STI na criação, edição e coordenação da implantação das políticas gerais da ferramenta de antivírus;

XI - o CDCAER poderá, junto a representantes dos ODGSA, assessorar o Órgão Central do STI na definição de cronogramas de implantação e atualização da ferramenta do antivírus no COMAER;

XII - cabe aos Elos de Serviço que possuírem servidores de antivírus descentralizados executarem o cronograma de implantação e atualização da ferramenta do antivírus nas OM

apoiadas;

XIII - o CDCAER poderá informar ao Órgão Central do STI e aos ODGSA o panorama de instalação e atualização da ferramenta de antivírus, para devidas providências em suas OM subordinadas;

XIV - cabe ao CDCAER acompanhar a disponibilidade dos servidores de antivírus no COMAER, bem como, notificar os responsáveis visando o restabelecimento do serviço;

XV - as OM que decidirem pela não utilização do antivírus em algum dispositivo de sua OM deverão informar a motivação ao Órgão Central do STI e serão responsáveis pelas ameaças decorrentes desta decisão;

XVI - é de responsabilidade da OM reportar ao CDCAER qualquer dificuldade de instalação e atualização do antivírus;

XVII - é responsabilidade da OM que possua algum servidor de antivírus descentralizado designar apoio técnico local com vistas a facilitar a comunicação com CDCAER; e

XVIII - o CDCAER deve possuir acesso de administrador em todos os servidores de antivírus.

ANEXO VI

POLÍTICA DE FIREWALL E RECURSOS COMPUTACIONAIS LOCALIZADOS EM ZONAS DESMILITARIZADAS

Art. 1º As Organizações do COMAER deverão adotar medidas de defesa em profundidade e configurar servidores de **firewall**, **IPS**/**IDS** (**Intrusion Prevention System**/**Intrusion Detection System**) e **WAF** (**Web Application firewall**) em suas redes de comunicação de dados locais e rede corporativa, conforme os seguintes requisitos:

I - o **firewall** deverá intermediar as comunicações entre as redes locais das OM e as demais (Internet, Intraer ou outras), minimizando incidentes de segurança e o uso abusivo;

II - o ponto de entrada e saída da rede das redes locais das OM deverá ser controlado e monitorado por IDS, configurado conforme os serviços prestados;

III - o **firewall** deverá ser configurado, por padrão, para bloquear todo e qualquer tráfego entre as redes, sendo posteriormente permitidos os acessos necessários para a utilização de serviços relacionados a execução de atividades funcionais;

IV - sempre que possível, deverão ser adotadas medidas de defesa em profundidade, utilizando mecanismos diversos para proteção contra falhas de defesa;

V - quando necessário liberar algum serviço para a Internet, este deverá ser disponibilizado em uma DMZ, com controles para proteção e monitoração de tentativas de invasão ou negação de serviço;

VI - os servidores de **firewall** internos, dedicados à comunicação entre as redes locais, as redes da DMZ e a Intraer, não devem ser os mesmos dos servidores de **firewall** externos, utilizados para permitir o acesso entras as redes da DMZ e a Internet;

VII - os servidores de **firewall** internos, dedicados à comunicação entre as redes locais, as redes da DMZ e a Intraer, devem ser de um fabricante diferente dos servidores de **firewall** externos, utilizados para permitir o acesso entras as redes da DMZ e a Internet;

VIII - os servidores de **firewall** dedicados à comunicação entre as redes locais, as redes da DMZ e a Intraer, não devem fornecer qualquer tipo de serviço, como VPN ou interfaces de administração WEB ou **desktop**, para redes externas à OM, como a Intraer, as redes da DMZ ou a Internet;

IX - a solução de IDS/IPS pode estar inclusa em uma solução de **firewall**;

X - sempre que o **firewall**, **IDS**, **IPS** ou **WAF** indicar um possível incidente de segurança, o administrador deverá notificar o CTIR.FAB através do **e-mail** abuse@fab.mil.br, com as evidências do evento suspeito;

XI - durante atividades realizadas pelo CDCAER que exijam acesso à rede local, as regras de **firewall** devem ser ajustadas para permitir este acesso;

XII - o CDCAER poderá propor bloqueios ou criação de assinaturas nas soluções de **firewall**, **IPS** e **WAF** ao tomar conhecimento de ameaças cibernéticas; e

XIII - ao liberar serviços para a Internet, Intraer ou outra rede externa à OM, esses serviços devem ser disponibilizados em uma DMZ, com controles necessários para proteção e monitoramento (**firewall**, **IPS**/**IDS** e **WAF**) de tentativas de invasão ou negação de serviço.

ANEXO VII
POLÍTICA DE SEGURANÇA FÍSICA

Art. 1º Todos os usuários de recursos computacionais do COMAER, ou terceiros, conectados ou não às redes locais de comunicação de dados de uma OM, devem observar os procedimentos descritos a seguir:

I - os equipamentos de conectividade (roteadores, **switches**, servidores e outros dispositivos de interconexão) deverão estar em salas exclusivas e com acesso restrito às equipes de TI das respectivas redes de comunicação de dados. Equipamentos e sistemas utilizados para a produção de documentos com grau de sigilo classificados somente poderão estar ligados a redes de computadores seguras e que sejam fisicamente e logicamente isoladas de qualquer outra, observando-se o disposto no ICA 205-47/2015;

II - estes equipamentos deverão possuir, na medida do possível, quadros de alimentação exclusivos que deverão permanecer trancados e com acesso restrito a pessoas habilitadas e com a devida ciência do Chefe da equipe de TI da OM;

III - as salas onde esses equipamentos estão localizados deverão ser providas de mecanismos de tranca e de controle de acesso pessoal, preferencialmente com reconhecimento biométrico; usuários não credenciados não poderão ter acesso a estes equipamentos;

IV - as salas onde esses equipamentos estão localizados deverão ser providas de mecanismos de monitoramento e controle ambiental de forma a minimizar ameaças potenciais como roubo, fogo, explosivos, fumaça, poeira, vibração, efeitos químicos, temperatura, umidade, dentre outros. Deve-se, ainda, manter as salas e os recursos computacionais limpos, organizados e conservados, sendo proibido o consumo de alimentos, bebidas, cigarros e similares nestes locais;

V - para a conexão de computadores ao **backbone**, sempre adotar switches ou equipamentos equivalentes que possibilitem o controle de portas;

VI - os recursos computacionais deverão passar por processo de manutenção preventiva periódica para evitar falhas de **hardware**. Todas as manutenções preventivas ou corretivas deverão ser documentadas para que haja um histórico dos problemas ocorridos e das respectivas soluções;

VII - caso haja necessidade da entrada de outra pessoa em salas de acesso restrito, que não dos membros das equipes locais de TI, ela deverá ser acompanhada por pelo menos um dos membros da referida equipe;

VIII - a alimentação elétrica para os recursos computacionais deverá ser exclusiva, constante e em níveis adequados ao funcionamento desses recursos, bem como possuir aterramento apropriado à proteção contra surtos e sobretensões, seguindo-se as recomendações fornecidas pelo fabricante de cada equipamento;

IX - os equipamentos de interconexão da rede local de cada OM devem estar alimentados por **no-break** com autonomia mínima de 20 (vinte) minutos a plena carga;

X - o cabeamento interno das redes locais, bem como os de interconexão entre redes, deverá estar encapsulado em conduítes e/ou calhas que o protejam de interrupções acidentais, e deverão estar identificados para que não sejam expostos indevidamente. O acesso ao cabeamento deverá somente ser permitido à pessoa autorizada e qualificada para tal;

XI - nenhum recurso computacional poderá ser movimentado sem o expresso consentimento dos detentores do material carga e com o conhecimento e aval do Chefe de TI da OM, para que o mesmo execute os procedimentos de segurança que forem necessários, em função da destinação do equipamento e dos dados nele armazenados, estabelecidos nesta Política; deve-se, ainda, manter um registro de entrada e saída contendo horário, data e nome do responsável pela movimentação destes recursos;

XII - a manutenção dos equipamentos, da rede de comunicação de dados locais das OM do COMAER, deverá ser feita preferencialmente nas dependências da própria organização à qual pertence o equipamento, com a supervisão de um ou mais membros da equipe de TI da OM;

XIII - quando qualquer equipamento necessitar ser retirado do seu local de origem, para manutenção, ou qualquer outro fim, que não seja o uso de um sistema nele contido, este deverá ter todos os arquivos (de configuração e/ou dados) apagados de forma segura, quer estejam em disco (usando técnicas para sobrescrever um disco para garantir que qualquer dado previamente existente torne-se completamente ilegível), memórias ou qualquer outro meio de armazenamento, para que o mesmo não comprometa a segurança interna da respectiva rede. Esta operação deverá ser executada quantas vezes forem necessárias, de forma a impossibilitar a recuperação de informações anteriormente armazenadas;

XIV - as OM do COMAER, através das suas equipes de TI, deverão manter um controle rígido sobre os usuários e os equipamentos que estão conectados às suas respectivas redes de comunicação de dados locais, de forma a impedir qualquer conexão de recursos computacionais não autorizados àquelas redes;

XV - as OM do COMAER, através das suas equipes de TI, deverão manter os seus recursos computacionais com os respectivos gabinetes lacrados, permitindo assim, constatar a ocorrência de possíveis violações. Estes equipamentos somente poderão ser abertos pelas equipes de TI responsáveis;

XVI - em caso de violação do lacre, a equipe de TI da OM deverá ser acionada para a execução de vistoria especializada. A não comunicação imediata da violação do lacre por parte do detentor da carga à equipe de TI da OM implica na sua responsabilização;

XVII - mídias de **backup** devem ser armazenadas em compartimentos à prova de fogo e água e separados fisicamente do local do sistema copiado, preferencialmente em outro prédio;

XVIII - as OM do COMAER deverão proteger todos os equipamentos de conexão de rede com dispositivo anti-roubo, desde que localizados em ambientes abertos;

XIX - no desligamento ou demissão de servidor civil ou afastamento do militar, solicitar a devolução de bens de propriedade da organização, condicionando esta devolução ao desimpedimento de sua ficha pelo setor de TI da OM e, consequentemente, sendo pré-requisito para o seu desligamento;

XX - todos os recursos computacionais deverão ser desligados no final de expediente de trabalho, quando não houver previsão de utilização dos mesmos; e

XXI - os servidores de rede, switches e outros equipamentos de conectividade existentes na Organização Militar do COMAER, deverão estar ligados 24 (vinte e quatro) horas por dia, sete dias por semana. Caso sejam desligados por motivos de manutenção programada ou força maior, os usuários deverão ser comunicados previamente.

ANEXO VIII
POLÍTICA DE SEGURANÇA DOS SERVIÇOS DE REDE

Art. 1º Na disponibilização dos serviços de rede deve ser observado o que se segue:

I - os servidores conectados à rede local, a princípio, são privativos para uso da comunidade de usuários interna, devendo estar protegidos contra acessos indevidos;

II - os servidores que disponibilizam serviços para a comunidade de usuários externa deverão estar na zona desmilitarizada (DMZ (**Demilitarized Zone**)), e sempre ser monitorados contra tentativas de invasão e negação de serviços;

III - cada serviço deverá ser disponibilizado em um ou mais servidores dedicados, sendo que este deverá, sempre que possível, comportar apenas um serviço;

IV - a responsabilidade pela manutenção dos serviços é do chefe da equipe de TI da OM que os hospedam;

V - serviços ou protocolos inseguros devem ser atualizados para suas versões mais recentes e seguras ou substituídos por equivalentes mais seguros, sempre que existirem, antes de serem disponibilizados na rede local da OM;

VI - o protocolo simples de gerência de rede, ou SNMP (**Simple Network Management Protocol**), é de uso exclusivo dos administradores de rede, dos membros da equipe de segurança da informação da OM, dos Elos Especializados do STI e do CTIR.FAB;

VII - o acesso ao serviço DNS deve ser limitado à consulta para a resolução de nomes. A transferência de zonas de domínio internas deverá ser somente para servidores secundários;

VIII - deve-se isolar o servidor DNS de rede local do servidor DNS de Internet, protegendo-o contra acessos externos à rede local da OM;

IX - o serviço de banco de dados deverá ter uma política específica, em conformidade com a Política de Manipulação de Informações Classificadas (Anexo IV);

X - em caso de comprometimento da segurança cibernética de um servidor, o incidente deve ser reportado para a ETIR responsável, e a equipe de TI da OM deve adotar os procedimentos sugeridos por aquela ETIR. Quando se tratar de crime envolvendo o espaço cibernético, todos os vestígios deverão ser preservados segundo orientações da ETIR para posterior realização de perícia forense digital em apoio ao tratamento de incidentes cibernéticos;

XI - todos os **softwares** dos recursos computacionais deverão estar atualizados com os **patches** mais recentes previamente testados em ambiente isolado;

XII - deverá ser definida pelo Órgão Central do STI uma topologia para implementação de um serviço de sincronização de relógios por meio de NTP (**Network Time Protocol**), para uso na Intraer;

XIII - a responsabilidade da manutenção, monitoração de funcionamento e segurança, bem como, da aplicação dos **patches** dos sistemas é do Chefe da equipe de TI da OM, no âmbito das suas respectivas sub-redes e domínios;

XIV - caso haja a necessidade de manutenções remotas, a possibilidade deve ser avaliada pela equipe responsável para cada caso, considerando os riscos envolvidos e as medidas de

segurança disponíveis;

XV - todos os servidores conectados à rede devem ser protegidos por **firewalls** que monitorem e filtrem o tráfego de rede, garantindo que apenas comunicações autorizadas e seguras sejam permitidas. O **firewall** deve ser configurado para bloquear todo o tráfego não autorizado e registrar tentativas de acesso indevido para auditoria;

XVI - deve-se garantir que todos os dispositivos de usuário final estejam protegidos por **firewalls** baseados em **host**, com regras de segurança que controlem o tráfego de entrada e saída. O **firewall** do dispositivo deve ser configurado para bloquear tentativas de conexão não solicitadas e alertar sobre atividades suspeitas;

XVII - para os servidores, o **firewall** deve ser configurado de forma a permitir apenas os serviços estritamente necessários para o funcionamento dos serviços e processos autorizados. Qualquer outro serviço não essencial deve ser bloqueado, e as portas desnecessárias devem ser fechadas;

XVIII - os **firewalls** instalados nos dispositivos de usuário final devem ser gerenciados centralmente, garantindo a aplicação consistente das políticas de segurança em toda a rede, e devem ser periodicamente atualizados para responder a novas ameaças de segurança; e

XIX - todas as regras de **firewall** devem ser revisadas e auditadas regularmente para garantir a conformidade com as melhores práticas de segurança e garantir que os ajustes necessários sejam realizados rapidamente para mitigar riscos emergentes

ANEXO IX
POLÍTICA DE SEGURANÇA EM SERVIDORES

Art. 1º Todos os servidores de rede do COMAER ou de terceiros, e que não sejam acessados externamente à rede local de uma OM devem obedecer aos procedimentos descritos abaixo:

I - todos os servidores devem ser gerenciados pelos administradores de rede locais, que devem manter manuais atualizados de configuração segura destas máquinas de maneira a refletir o descrito nesta Política;

II - servidores corporativos devem ser configurados para carregar seus sistemas exclusivamente a partir do disco rígido interno. Todos os outros meios que puderem ser usados para a carga do sistema devem ser desabilitados, exceto em situações temporárias necessárias e definidas pelo Chefe da equipe de TI da OM;

III - não devem existir múltiplas contas de acesso ao servidor para um mesmo usuário, com exceção dos administradores de rede local. Contas padrão como root e administrador, quando não utilizadas, devem ser desativadas;

IV - nenhum programa deve ser executado no servidor pelo usuário a partir de uma estação de trabalho, exceto aqueles definidos e permitidos claramente pelo administrador de rede local;

V - as sessões de uma estação de trabalho devem ser suspensas pelo administrador de rede local após um período de inatividade, e encerradas após um período pré-determinado depois do tempo esgotado, de acordo com o previsto na Política de Administração de Recursos Computacionais (Anexo III);

VI - todas as funções de segurança e as alterações e inclusões de **software** devem ser feitas a partir do servidor e apenas pelo administrador de rede local;

VII - o acesso físico ao servidor via console não deve ser uma prática rotineira. O acesso lógico de usuários ao servidor, após as devidas configurações de acessibilidade, deverá ser somente através da rede. O mesmo deve ser realizado somente por protocolos de acesso seguros como SSH, RDP;

VIII - os arquivos classificados devem ser mantidos criptografados segundo a Política de Manipulação de Informações Classificadas (Anexo IV). Isto inclui arquivos de senha, arquivos-chave e arquivos com dados confidenciais;

IX - todas as transações devem ser registradas, tais como as tentativas de entrada mal sucedidas no sistema, operação/acesso não autorizados, suspensão e encerramento de sessão (acidental ou deliberada), mudanças na atribuição de **software** e de segurança, entrada/saídas do sistema (**logons/logoffs**), outras atividades designadas (por exemplo, acessos aos arquivos classificados) e, opcionalmente, todas as atividades, pelo período mínimo descrito na Política de Gestão de Registros (**Logs**) de Auditoria – PGRA (Anexo XVII).

X - os usuários devem possuir diretórios próprios para armazenamento de arquivos;

XI - não devem ser transferidos programas e arquivos para as áreas públicas; o mesmo vale para as macros e bibliotecas de macros, salvo necessidade de divulgação pública e o referido programa ou arquivo não venha a comprometer a segurança do servidor ou da rede local da OM;

XII - caso seja necessário, um procedimento adicional de identificação de usuários poderá ser usado, dependendo das informações a serem acessadas;

XIII - os servidores corporativos devem estar registrados em um documento mantido em poder dos Chefes da equipe de TI das respectivas OM, contendo no mínimo as seguintes informações: a localização do servidor; o contato do administrador de rede local; o **hardware** do servidor; a versão do sistema operacional e **softwares** instalados; a função principal a que se destina;

XIV - alterações de configurações de servidores em operação devem seguir os procedimentos padronizados e documentados de acordo com o planejamento estabelecido pela equipe de TI da OM;

XV - serviços e aplicações que não serão usados devem ser desabilitados ou desinstalados do servidor sempre que possível;

XVI - acessos aos serviços devem ser registrados e protegidos;

XVII - relações de confiança entre sistemas oferecem riscos à segurança e, portanto, devem ser substituídas, sempre que possível, por outros métodos mais seguros de comunicação;

XVIII - os servidores de rede devem estar fisicamente localizados em ambientes de acesso controlado, conforme definido na Política de Segurança Física (Anexo VII);

XIX - quando da instalação de um novo servidor, roteador ou switch, as senhas originais devem ser substituídas, assim como as contas padrões devem ser renomeadas ou desativadas;

XX - os eventos relacionados à segurança devem ser reportados à Equipe de Tratamento de Incidentes (ETIR) de referência da OM por meio do **e-mail** abuse@fab.mil.br, contendo evidências do evento suspeito;

XXI - bloquear a execução de scripts nos servidores, exceto aqueles analisados e autorizados pelo administrador da rede local. Esta premissa pode ser reavaliada com frequência, no mínimo, semestral. O bloqueio é motivado pela possibilidade de impacto na disponibilidade, autenticidade e integridade dos sistemas hospedados no respectivo servidor, necessitando de análise cuidadosa pelo administrador da rede local; e

XXII - o sistema operacional dos servidores deve ser atualizado sempre que houver novas versões disponíveis que sejam compatíveis com os serviços em execução.

ANEXO X
POLÍTICA DE ACESSO REMOTO

Art. 1º Todos os usuários que necessitem utilizar acessos remotos a uma rede local de uma OM, devidamente autorizados pelo Elo de Coordenação do ODGSA, observadas as regras emanadas pelo Órgão Central do STI, devem observar os procedimentos descritos a seguir:

I - as implementações de acesso remoto coberto por esta Política incluem, mas não se limitam a serviços, tais como, modems, ISDN (**Integrated Service Digital Network**), **frame relay**, VPN (**Virtual Private Network**) e SSH (**Secure Shell**);

II - somente serão permitidos acessos remotos à Intraer através de conexões passando pelos **firewalls** corporativos e locais, devendo ser obrigatoriamente registrados e mantidos pelo período mínimo estabelecido na Política de Gestão de Registros (**Logs**) de Auditoria – PGRA (Anexo XVII);

III - não é permitido que de equipamentos da rede local de uma OM originem-se conexões de redes que não sejam controladas pelos **firewalls** corporativos, tais como acesso discado, wireless e equivalentes;

IV - o acesso remoto à rede local de uma OM deve ser, obrigatoriamente, controlado através de um esquema de autenticação forte como códigos e senhas com validade, chaves públicas e autenticação multifator (MFA);

V - não serão permitidos os acessos remotos provenientes de redes externas à rede local de uma OM, bem como aos recursos computacionais, através de contas com privilégios de administrador, supervisor ou superusuário. O acesso, como administrador, supervisor ou superusuário, só poderá ser feito via console ou através da rede local de uma OM por intermédio de um protocolo seguro utilizando criptografia forte;

VI - para a devida proteção de informações e detalhes de uso aceitável quando acessando a rede local de uma OM, deve-se seguir o previsto na Política de Uso de Recursos Computacionais (Anexo II) e na Política de Manipulação de Informações Classificadas (Anexo IV);

VII - todo acesso remoto deve utilizar-se de algoritmos criptográficos, de acordo com o expresso no Anexo II;

VIII - não é permitido realizar acesso discado a sistemas internos ou externos, exceto quando, para atender uma necessidade excepcional e temporária, esse acesso seja justificado e devidamente autorizado pelo Elo de Coordenação de TI do ODGSA envolvido, observados os requisitos emanados pelo Órgão Central do STI; e

IX - o uso de tecnologias baseadas em propagação de ondas eletromagnéticas, em rede, deve ser autorizado pelo Elo de Coordenação de TI do ODGSA, observadas as regras emanadas pelo Órgão Central do STI.

ANEXO XI
POLÍTICA DE SEGURANÇA LÓGICA

Art. 1º Todos os recursos computacionais utilizados no COMAER, corporativos ou de terceiros, conectados ou não à rede local de uma OM, que mantenham ou não dados importantes e/ou classificados, devem observar os procedimentos descritos a seguir:

I - para ter acesso ao serviço disponibilizado pelas redes de dados locais e pela Intraer, o usuário necessita ser cadastrado e a partir de então, identificar-se através de uma conta de usuário e uma senha;

II - o nível de acesso aos arquivos (programas e dados), quanto à leitura, escrita e execução, deve ter uma atribuição individual, por grupo ou pública, definida conforme a necessidade de cada usuário ou grupo de usuários, no momento da abertura da conta de acesso aos recursos computacionais disponibilizados nas referidas redes;

III - o acesso aos recursos computacionais somente deverá ser feito pelo usuário quando necessário e expressamente autorizado pelo Comandante, Chefe ou Diretor e pela sua Chefia funcional;

IV - a permissão de acesso total ou equivalente deve ser removida dos diretórios compartilhados nos recursos computacionais utilizados como servidores, salvo aqueles que deverão ser disponibilizados ao público externo nos servidores alocados na DMZ, com a permissão única de leitura;

V - o controle de acesso aos dados armazenados deve ser definido tanto em nível de arquivos como de diretórios, devendo ser usada a política de menor privilégio necessário, ou seja, cada usuário deve ter apenas o nível de acesso e privilégio suficiente para a execução de suas atividades;

VI - as OM do COMAER, por meio das suas equipes de TI, deverão providenciar as cópias de segurança das informações armazenadas em cada servidor sob sua responsabilidade, com o intuito de prover uma recuperação rápida de dados armazenados em caso de falha ou interrupção de algum serviço;

VII - as cópias de segurança não deverão, em hipótese alguma, ser armazenadas no mesmo espaço físico do servidor e no mesmo prédio. A periodicidade das cópias deverá ser baseada no seu grau de criticidade para operações do dia-a-dia, podendo exigir, conforme o entendimento do Elo de Coordenação de TI respectivo, periodicidade diária, semanal ou mensal;

VIII - o agendamento do processo de execução das cópias de segurança deverá ser feito, obrigatoriamente, pela equipe de TI da OM;

IX - a disponibilidade da rede deve ser mantida fazendo-se cópias de segurança programadas e regulares. Todos os recursos de segurança, atributos e diretórios, devem ser respeitados e mantidos pelo procedimento de cópias de segurança;

X - tanto as cópias quanto as funções de recuperação devem ser testadas regularmente;

XI - se um sistema de controle de acesso falhar, este deve negar todos os privilégios aos usuários até a eliminação da falha;

XII - para os sistemas isolados, o usuário será o responsável pelo processo de execução das cópias de segurança, enquanto para sistemas multiusuários, a equipe de TI da OM será a responsável;

XIII - todas as informações classificadas, sensíveis, valiosas ou críticas armazenadas nos recursos computacionais e em uma rede deverão ser periodicamente copiadas, baseando-se no seu grau de criticidade para operações do dia-a-dia, podendo exigir, periodicidade diária, semanal ou mensal; e

XIV - o armazenamento do conjunto de mídias de **backup** de servidores é de responsabilidade da equipe de TI da OM, assim como o das estações de trabalho é de responsabilidade do usuário.

ANEXO XII
POLÍTICA DE INSPEÇÃO

Art. 1º Na condução de inspeção de segurança em recursos computacionais do COMAER devem ser observados os seguintes critérios:

I - todos os recursos computacionais pertencentes à Intraer, bem como os recursos computacionais das OM deverão sofrer inspeções para verificação da implementação e cumprimento de Segurança, com a ciência prévia do Comando/Chefia/Direção da OM onde eles estejam localizados;

II - o CDCAER poderá inspecionar as organizações a qualquer tempo, com fins de promover o incremento da Ptç Ciber através da busca de vulnerabilidades. Poderá aplicar técnicas, táticas e procedimentos de exploração manual ou automatizada, sem necessidade de autorização da OM, nem necessidade de comunicação prévia, durante ou posterior;

III - quando necessário, ou com o propósito de ser executada a inspeção, equipe de segurança em TI da OM e do CDCAER deverão ter acesso irrestrito aos recursos computacionais, com a ciência do Comando/Direção/Chefia da organização inspecionada;

IV - os inspetores terão acesso a todas as informações, sejam elas eletrônicas, cópias de segurança e outras, que possam ter sido transmitidas, produzidas ou armazenadas nos recursos computacionais da organização inspecionada, devendo ser levada em consideração a credencial de segurança dos inspetores;

V - os inspetores terão acesso a todas as áreas de trabalho onde se encontram os recursos computacionais, tais como laboratórios, salas diversas, manutenção e outras;

VI - os inspetores terão acesso físico e lógico aos sistemas que monitoram e armazenam os **logs** da rede;

VII - a inspeção deverá ser feita com aviso prévio ao Chefe da equipe de TI da OM e este, além de manter sigilo sobre o processo, deverá acompanhar os inspetores em todos os procedimentos executados;

VIII - conforme atribuições previstas na NSCA 7-6/2016 e na ICA 7-60/2024, o CDCAER, por meio do CTIR.FAB e de suas demais seções, poderá manter um monitoramento remoto constante da Intraer em qualquer ponto do **backbone**, incluindo redes locais, sem necessidade de prévio aviso a qualquer usuário;

IX - todo esforço deverá ser feito para impedir que as inspeções causem falhas operacionais ou interrupção dos serviços;

X - todo recurso computacional existente no COMAER é passível de monitoramento e inspeção pelo CDCAER, conforme atribuições previstas na NSCA 7-6/2016 e na ICA 7-60/2024; e

XI - considerando que os recursos computacionais são de propriedade do COMAER ou estão sendo utilizados em atividades desenvolvidas em seu benefício, entende-se que o usuário não possui qualquer expectativa de privacidade no uso desses recursos.

ANEXO XIII
POLÍTICA DE BACKUP E RESTAURAÇÃO DE DADOS DIGITAIS

CAPÍTULO I
PROPÓSITO

Art. 1º Esta Política de Backup e Restauração de Dados Digitais institui diretrizes, responsabilidades e competências que visam à segurança, proteção e disponibilidade dos dados digitais custodiados pelos Elos do STI e formalmente definidos como de necessária salvaguarda no COMAER, para se manter a continuidade do negócio.

Art. 2º Nela são estabelecidos mecanismos com o objetivo de permitir a guarda dos dados e sua eventual restauração em casos de indisponibilidades ou perdas por erro humano, ataques, catástrofes naturais ou outras ameaças.

CAPÍTULO II
ESCOPO

Art. 3º Esta Política se aplica a todos os dados no âmbito da COMAER, incluindo dados fora da estrutura do STI ou armazenados em um serviço de nuvem Pública ou Privada. “Dados críticos”, neste contexto, incluem **e-mail**, arquivos pessoais e compartilhados, bancos de dados, **logs** de sistemas, conteúdos disponibilizados em páginas web e sistemas operacionais.

Art. 4º Esta política se aplica a todos que podem ser criadores e/ou usuários de tais dados e a todos, incluindo terceiros, que acessam e usam no COMAER sistemas e equipamentos de TI ou que criam, processam ou armazenam dados de propriedade do COMAER.

Art. 5º Não serão salvaguardados nem recuperados dados armazenados localmente, nos microcomputadores dos usuários ou em quaisquer outros dispositivos fora dos Elos do STI, ficando sobre a responsabilidade do indivíduo que usa o(s) dispositivo(s).

Art. 6º A salvaguarda dos dados em formato digital pertencentes a serviços de TI do COMAER, mas custodiados por outras entidades, públicas ou privadas, como nos casos de serviços em nuvem, deve estar garantida nos acordos ou contratos que formalizam a relação entre os envolvidos.

CAPÍTULO III
DECLARAÇÕES DA POLÍTICA

Art. 7º Este documento estabelece as regras prescritivas e proscritivas para a execução da Política de Backup e Restauração de Dados Digitais no COMAER, com o intuito de garantir a proteção, integridade e disponibilidade dos dados, além de assegurar a continuidade das operações essenciais da organização.

Art. 8º As regras aqui descritas são obrigatórias e devem ser seguidas por todos os envolvidos nos processos de TI, desde os responsáveis pela execução dos **backups** até os gestores que devem garantir o cumprimento da política.

Seção I
Dos princípios gerais

Art. 9º Esta Política de Backup e Restauração de Dados deve permanecer alinhada com a Política de Segurança da Informação do COMAER.

Art. 10. Esta Política deve permanecer alinhada com a gestão de continuidade de negócios em nível organizacional.

Art. 11. As rotinas de **backup** devem:

I - ser orientadas para a restauração dos dados no menor tempo possível, principalmente quando da indisponibilidade de serviços de TI;

II - utilizar soluções próprias e especializadas para este fim, preferencialmente de forma automatizada; e

III - possuir requisitos mínimos diferenciados de acordo com o tipo de serviço de TI ou dado salvaguardado, dando prioridade aos serviços de TI críticos da organização.

Art. 12. O armazenamento de **backup**, se possível, deve ser realizado em um local distinto da infraestrutura crítica.

Parágrafo único. É desejável que se tenha um sítio de **backup** em um local remoto ao da sede da organização para armazenar cópias extras dos principais **backups**, a exemplo dos **backups** de dados de serviços críticos.

Art. 13. A infraestrutura de rede de **backup** deve ser apartada, lógica e fisicamente, dos sistemas críticos da organização.

Art. 14. Os Elos do STI devem manter reserva de recursos (físicos e lógicos) de infraestrutura para realização de teste de restauração de **backup**.

Art. 15. Em situações em que a confidencialidade é importante, as cópias de segurança devem ser protegidas através de encriptação.

Seção II
Da frequência e retenção dos dados

Art. 16. Os **backups** dos serviços de TI críticos do COMAER devem ser planejados de acordo com o sistema, a área de negócio atendida e os recursos disponíveis, com base nas seguintes frequências temporais, devendo ser registrados nos acordos de níveis de serviço (ANS):

I - diária;

II - semanal;

III - mensal; e/ou

IV - anual.

Art. 17. Os serviços de TI críticos do COMAER devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: 2 meses;

II - semanal: 4 meses;

III - mensal: 1 ano; e/ou

IV - anual: 5 anos.

Art. 18. Os serviços de TI NÃO críticos do COMAER devem ser resguardados sob um padrão mínimo, o qual deve observar a correlação frequência/retenção de dados estabelecida a seguir:

I - diária: 1 meses;

II - semanal: 2 meses;

III - mensal: 6 meses; e/ou

IV - anual: 2 anos.

Art. 19. Especificidades dos serviços de TI críticos e dos serviços de TI não críticos podem demandar frequência e tempo de retenção diferenciados.

Art. 20. Os ativos envolvidos no processo de **backup** são considerados ativos críticos para a organização.

Art. 21. A solicitação de salvaguarda dos dados referentes aos serviços de TI críticos e aos serviços de TI não críticos deve ser realizada pelo Gerente de Negócio da Solução de TI, com a anuência prévia e formal do Órgão Central do STI, refletindo os requisitos de negócio da organização, bem como os requisitos de segurança da informação e proteção de dados envolvidos e a criticidade da informação para a continuidade da operação da organização, e deve explicitar, no mínimo, os seguintes requisitos técnicos:

I - escopo (dados digitais a serem salvaguardados);

II - tipo de **backup** (completo, incremental, diferencial);

III - frequência temporal de realização do **backup** (diária, semanal, mensal, anual);

IV - retenção;

V - RPO; e

VI - RTO.

Art. 22. A alteração das frequências e tempos de retenção definidos nesta seção deve ser precedida de solicitação e justificativa formais encaminhadas ao Elos do STI que atua como Órgão Operador da Solução de TI, responsável pelo **backup**.

Parágrafo único. A aprovação para execução da alteração depende da anuência do Órgão Central do STI.

Art. 23. Os responsáveis pelos dados deverão ter ciência dos tempos de retenção estabelecidos para cada tipo de informação e os administradores de **backup** deverão zelar pelo cumprimento das diretrizes estabelecidas.

Seção III
Do tipo de backup

Art. 24. Os tipos de **backup** possíveis são:

I - completo (**full**);

II - incremental; e

III - diferencial.

Art. 25. Salvo indicação em contrário, o **backup** dos dados do sistema será feito de acordo com a seguinte programação padrão:

I - o **backup** diário será preferencialmente do tipo incremental e será realizado de segunda a sábado; e

II - os **backups** semanais serão preferencialmente do tipo diferencial, e serão realizados de sábado a domingo, sendo iniciados, sempre que possível, às 12h da manhã de sábado para permitir mais tempo durante o fim de semana para realizar o **backup** e tempo suficiente para lidar com quaisquer problemas que possam surgir durante o processo de **backup**.

Seção IV
Do uso da rede

Art. 26. O administrador de **backup** deve considerar o impacto da execução das rotinas de **backup** sobre o desempenho da rede de dados do COMAER, garantindo que o tráfego necessário às suas atividades não ocasione indisponibilidade dos demais serviços de TI do COMAER.

Art. 27. A execução do **backup** deve concentrar-se, preferencialmente, no período de janela de **backup**.

Art. 28. O período de janela de **backup** deve ser determinado pelo administrador de **backup** em conjunto com a equipe técnica responsável pela administração da rede de dados.

Seção V
Do transporte e armazenamento

Art. 29. As unidades de armazenamento utilizadas na salvaguarda dos dados digitais devem considerar as seguintes características dos dados resguardados:

I - a criticidade do dado salvaguardado;

II - o tempo de retenção do dado;

III - a probabilidade de necessidade de restauração;

IV - o tempo esperado para restauração;

V - o custo de aquisição da unidade de armazenamento de **backup**;

VI - a vida útil da unidade de armazenamento de **backup**.

Art. 30. O administrador de **backup** deve identificar a viabilidade de utilização de diferentes tecnologias na realização das cópias de segurança, propondo a melhor solução para cada caso.

Art. 31. Podem ser utilizadas técnicas de compressão de dados, contanto que o acréscimo no tempo de restauração dos dados seja considerado aceitável pelos gestores das informações.

Art. 32. A execução das rotinas de **backup** deve envolver a previsão de ampliação da capacidade dos dispositivos envolvidos no armazenamento.

Art. 33. No caso de desligamento do usuário (de forma permanente ou temporária), o **backup** de seus arquivos em nuvem deverá ser mantido por, no mínimo, 30 dias. Após esse período os arquivos poderão ser excluídos a qualquer tempo.

Art. 34. As unidades de armazenamento dos **backups** devem ser acondicionadas em locais apropriados, com controle de fatores ambientais sensíveis, como umidade, temperatura, poeira e pressão, e com acesso restrito a pessoas autorizadas pelo administrador de **backup**. Além disso, as condições de temperatura, umidade e pressão devem ser aquelas descritas pelo fabricante das unidades de armazenamento.

Art. 35. Quando da necessidade de descarte de unidades de armazenamento de **backups**, tais recursos devem ser fisicamente destruídos de forma a inutilizá-los, atentando-se ao descarte sustentável e ambientalmente correto.

Art. 36. As fitas de **backup** serão transportadas e armazenadas, conforme descrito no padrão ISO/IEC 27002 (2022).

Art. 37. A mídia será claramente identificada e armazenada em uma área segura acessível apenas para pessoal autorizado.

Art. 38. A mídia não será deixada sem supervisão durante o transporte.

Seção VI
Dos testes de backup

Art. 39. Os **backups** serão verificados periodicamente:

I - os **logs** de **backup** serão revisados em busca de erros, durações anormais e em busca de oportunidades para melhorar o desempenho do **backup**, com a seguinte periodicidade:

a) diariamente para sistemas críticos; e

b) semanalmente para sistemas não críticos.

II - ações corretivas serão tomadas quando os problemas de **backup** forem identificados, a fim de reduzir os riscos associados a **backups** com falha;

III - a TI manterá registros de **backups** e testes de restauração para demonstrar conformidade com esta política; e

IV - os testes devem ser realizados em todos os **backups** produzidos independente do ambiente.

Art. 40. Os testes de restauração dos **backups** devem ser realizados, por amostragem em equipamentos servidores diferentes dos equipamentos que atendem os ambientes de produção, observados os recursos humanos de TI e tecnologias disponíveis, a fim de verificar **backups** bem-sucedidos, com a seguinte periodicidade:

I - semanalmente para sistemas críticos; e

II - mensalmente para sistemas não críticos.

Art. 41. Verificar se foi atendido os níveis de serviço pactuados, tais como os **Recovery Time Objective** – RTOs.

Art. 42. Os registros deverão conter, no mínimo, o tipo de sistema/serviço que teve o seu reestabelecimento testado, a data da realização do teste, o tempo gasto para o retorno do **backup** e se o procedimento foi concluído com sucesso

Art. 43. Quaisquer exceções a esta política serão totalmente documentadas e aprovadas pelo CGDSIPD.

Seção VII
Do procedimento de restauração de backup

Art. 44. O atendimento de solicitações de restauração de arquivos, **e-mails** e demais formas de dados deverá obedecer às seguintes orientações:

I - a solicitação de restauração de objetos deverá sempre partir do responsável pelo recurso, através de chamado SAU;

II - a restauração de objetos somente será possível nos casos em que este tenha sido atingido pela estratégia de **backup**;

III - a solicitação de restauração de dados que tenham sido salvaguardados depende de prévia e formal autorização dos respectivos gestores das informações; e

IV - o operador de **backup** terá a prerrogativa de negar a restauração de dados cujo conteúdo não seja condizente com a atividade institucional, cabendo recurso da negativa ao gestor da unidade do demandante.

Art. 45. O cronograma de restauração de dados deve ser elaborado conforme Acordo de Nível de Serviço (ANS) entre as áreas de negócio e de TIC.

§ 1º O ANS deve firmar o tempo de restauração deve ser proporcional ao volume de dados necessários para o **restore**.

§ 2º O ANS deve firmar o tempo em que **backups** externos serão disponibilizados depois de uma falha catastrófica do sistema, observando a prioridade para restauração de acordo com a criticidade de cada um.

Seção VIII
Do descarte da mídia

Art. 46. A mídia de **backup** será retirada e descartada conforme descrito neste documento:

I - a TI garantirá que a mídia não contenha mais imagens de **backup** ativas e que o conteúdo atual ou anterior não possa ser lido ou recuperado por terceiros não autorizados.

II - a TI garantirá a destruição física da mídia antes do descarte.

III - o descarte da mídia deve respeitar os procedimentos para Desfazimento de Bens de TI no COMAER.

Seção IX
Das responsabilidades

Art. 47. O administrador de **backup** e o operador de **backup** devem ser capacitados para as tecnologias, procedimentos e soluções utilizadas nas rotinas de **backup**.

Art. 48. O administrador de **backup** é o chefe do setor responsável pelos procedimentos de **backup** no Elo do STI responsável por cada escopo de atuação.

Art. 49. São atribuições do administrador de **backup**:

I - garantir a formalização das regras de **backup** em Acordo de Nível de Serviço (ANS);

II - propor soluções de cópia de segurança das informações digitais corporativas produzidas ou custodiadas pela organização;

III - providenciar a criação e manutenção dos **backups**;

IV - configurar as soluções de **backup**;

V - manter as unidades de armazenamento de **backups** preservadas, funcionais e seguras; e

VI - definir os procedimentos de restauração e neles auxiliar;

ANEXO XIV
POLÍTICA DE GESTÃO DE ATIVOS

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo desta política é garantir que os ativos de informação sejam identificados adequadamente e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Art. 2º Para manter a segurança e continuidade do negócio do COMAER, em sua missão deve-se mapear e monitorar os ativos tecnológicos, para maior controle da organização, auxiliando na aplicação de atualizações, implementação de controles de segurança e gestão de risco da organização, auxiliando também na recuperação de incidentes.

Art. 3º Os ativos de informação do COMAER devem ser classificados a fim de permitir a definição de níveis de segurança para eles. Cada ativo de informação deverá ter um "dono", no qual realizará a classificação do ativo de informação e deverá ser registrado em uma base de dados gerenciada de forma centralizada.

Art. 4º A base de dados centralizada para registro dos ativos de informação é o do Módulo de Gestão de Ativos de TI (GATI) do SILOMS.

Parágrafo único. Poderão ser utilizadas como facilitadoras, outras soluções de TI.

CAPÍTULO II
ESCOPO

Art. 5º Esta Política se aplica a todos os ativos de informação do COMAER, incluindo os ativos fora do COMAER armazenados em um serviço de nuvem. Ativos de informação neste contexto, incluem Documentos, base de dados, contratos, documentação de sistemas, procedimentos, manuais, **logs** de sistemas, planos, guias, programas de computador, servidores, computadores, **e-mail**, arquivos pessoais e compartilhados, bancos de dados e conteúdos disponibilizados em páginas web.

Parágrafo único. A classificação dos ativos de informação e o escopo desta política serão revisados anualmente.

CAPÍTULO III
DOS PRINCÍPIOS GERAIS

Art. 6º A Política de Gestão de Ativos de informação deve permanecer alinhada com a Política de Segurança da Informação do COMAER e ao Programa de Privacidade e Segurança da Informação (PPSI) do Governo Federal.

Art. 7º A Política de Gestão de Ativos de informação deve permanecer alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 8º O processo de mapeamento de ativos de informação deve 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 nos aspectos relativos à segurança da informação.

Art. 9º As rotinas de inventário e mapeamento de ativos de informação devem ser orientadas para a identificação dos ativos de informação da organização, a fim de manter o escopo da organização mapeado e documentado.

Art. 10. O processo de mapeamento de ativos de informação deve considerar, preliminarmente os objetivos estratégicos da organização, seus processos internos, os requisitos legais e sua estrutura organizacional.

Art. 11. O registro de ativos de informação resultante do processo de mapeamento de ativos de informação deverá conter: os responsáveis (proprietários e custodiantes) de cada ativo de informação; as informações básicas sobre os requisitos de segurança da informação de cada ativo de informação; os contêineres de cada ativo de informação; as interfaces de cada ativo de informação e as interdependências entre eles.

Art. 12. Todos os ativos deverão ser gerenciados durante todo o seu ciclo de vida.

Art. 13. Os seguintes ativos de informação devem ser considerados no processo de mapeamento de ativos de informação:

I - ativos físicos;

II - bancos de dados;

III - dispositivos móveis;

IV - **hardwares**;

V - mídias removíveis;

VI - níveis de permissões;

VII - procedimentos (processos mapeados);

VIII - serviços; e

IX - **softwares**.

CAPÍTULO IV
DAS DIRETRIZES

Art. 14. Informações ou ativos de informação de instalações de processamento de informações devem ser inventariados e documentados e esse registro deve ser mantido atualizado.

Art. 15. Os elos do STI devem utilizar da segmentação de rede para organizar ativos de informação sob sua guarda.

Art. 16. Os elos do STI devem implementar o controle de acessos e privilégios mínimos para a administração dos ativos de informação.

Art. 17. O Órgão Central do STI deve implementar, em um dos Elos Especializados, a centralização de autenticação, autorização e auditoria (AAA) para a administração de seus ativos de informação, principalmente os ativos que fazem parte da infraestrutura de rede do COMAER.

Art. 18. Alterações na categorização do inventário devem ser aprovadas pelo Órgão Central do STI.

Art. 19. Os Elos do STI devem adotar e fazer cumprir os níveis mínimos de disponibilidade de seus ativos de informação.

Art. 20. Os Elos do STI devem empregar o uso de mecanismos automatizados para identificar sistemas autorizados e não autorizados, incluindo **hardware** ou **software**.

Art. 21. Os Elos do STI devem assegurar que os ativos de informação inventariados possuam contrato de suporte em vigor.

Art. 22. Os Elos do STI devem empregar o uso de ferramentas de descoberta ativa e/ou passiva para identificar dispositivos conectados à rede da instituição e automaticamente atualizar o inventário de ativos.

Art. 23. Os Elos do STI devem utilizar ferramentas de inventário de **software**, quando possível, em seu escopo de atuação para automatizar a descoberta e documentação do **software** instalado.

Art. 24. Os Elos do STI devem assegurar que exista um processo semanal para lidar com ativos não autorizados.

Art. 25. Os Elos do STI devem utilizar controles técnicos em todos os ativos para garantir que apenas **software** autorizado seja executado, sendo estes reavaliados semestralmente ou com mais frequência.

Art. 26. Os Elos do STI devem utilizar controles técnicos para garantir que apenas bibliotecas e **scripts** autorizados, e assinados digitalmente tenham permissão para serem executados.

Art. 27. Os Elos do STI devem utilizar de **scripts** e protocolos de segurança para o acesso e administração dos ativos de informação.

Art. 28. O Órgão Central e os Elos do STI devem elaborar e manter diagramas e demais documentações da arquitetura de rede da organização no Módulo GATI do SILOMS. A revisão destas documentações deverá ser realizada de forma periódica ou quando ocorrerem mudanças significativas, que possam impactar tais artefatos.

Art. 29. Os Elos do STI devem garantir que as infraestruturas de rede de seu escopo de atuação estejam atualizadas. Deverá ser realizada uma revisão das versões de **software** de forma periódica, ou quando for identificada uma vulnerabilidade que eleve o risco da organização.

Art. 30. O inventário também deverá incluir atualizações ou remoções dos **softwares**, bem como dos sistemas de informação.

Art. 31. As atualizações e novas versões de **softwares** devem ser avaliadas e aprovadas antes da instalação.

Art. 32. Os Elos do STI devem utilizar ferramenta de gerenciamento de endereços IP - ex.: **Dynamic Host Configuration Protocol** *(*DHCP*)* - para atualizar o inventário de ativos em seu escopo de atuação.

Art. 33. Cada ativo de informação (por exemplo, **desktops**, **laptops**, servidores, **tablets**), quando aplicável, deve ter uma etiqueta afixada ao dispositivo com o número identificador do ativo e o número BMP.

Art. 34. O identificador de ativos da informação juntamente com outras informações relevantes no inventário de TI deve ser registrado. Isso inclui:

I - identificador de ativos;

II - data da compra;

III - preço de compra;

IV - descrição do item;

V - fabricante;

VI - número do modelo;

VII - número de série;

VIII - nome do proprietário do ativo corporativo (por exemplo, administrador, usuário), função ou unidade de negócios, quando aplicável;

IX - localização física detalhada do ativo, quando aplicável, incluindo:

a) nome da Organização;

b) sala;

c) rack, quando aplicável; e

d) servidor, quando aplicável.

X - endereço físico (controle de acesso à mídia (MAC));

XI - endereço de protocolo de Internet (IP);

XII - data de validade da garantia/vida útil;

XIII - qualquer informação de licenciamento relevante; e

XIV - no caso de **softwares** instalados na organização deve ser registrado no inventário informações como:

a) título do **software**;

b) desenvolvedor ou editor de **software**;

c) data de aquisição;

d) data de instalação;

e) duração do uso;

f) finalidade comercial;

g) lojas de aplicativos;

h) versões;

i) mecanismo de implantação;

j) data de fim do suporte, se conhecida;

k) qualquer informação de licenciamento relevante; e

l) data de descomissionamento.

Art. 35. O CTIR.FAB deverá ter acesso a todas as soluções de TI que sejam empregadas na atividade de Gestão de Ativos no COMAER.

CAPÍTULO V
DAS RESPONSABILIDADES DO PROPRIETÁRIO DO PROCESSO

Art. 36. O proprietário do processo é responsável por assegurar que os ativos de informação estejam devidamente protegidos e geridos, conforme estabelecido nesta Política.

Art. 37. O proprietário do processo de Gestão de Ativos do COMAER é o Órgão Central do STI.

Art. 38. É responsabilidade do proprietário do processo:

I - identificar potenciais ameaças aos ativos de informação;

II - identificar vulnerabilidades dos ativos de informação;

III - consolidar informações resultantes da análise do nível de segurança da informação de cada ativo de informação ou de grupos de ativos de informação em um relatório; e

IV - avaliar os riscos dos ativos de informação ou do grupo de ativos de informação.

Art. 39. Indivíduos que requerem acesso aos sistemas de informação devem seguir o procedimento adequado para receber tal acesso, como descritos na Política de Controle de Acesso e catalogadas no sistema de gestão de ativos.

Art. 40. Os processos em torno do gerenciamento de mudança e de configuração também serão estabelecidos e monitorados.

Art. 41. Todos os ativos de informação devem ser devolvidos após a rescisão do contrato de trabalho ou contrato.

CAPÍTULO VI
CRITICIDADE DO ATIVO DE INFORMAÇÃO

Art. 42. A criticidade dos ativos de informação críticos da organização é determinada com base nos seguintes aspectos:

I - requisitos legais;

II - nível básico de disponibilidade;

III - pelo valor financeiro;

IV - pelo seu potencial de agregar valor ao negócio;

V - por seu ciclo de vida útil;

VI - pela atividade que apoia diretamente sua missão;

VII - pela falha que pode ocasionar transtornos ou perdas econômicas significativas, por danos físicos ou ameaças aos seres humanos e ao meio ambiente;

VIII - pela privacidade das informações pessoais; e

IX - por outros critérios de risco.

Art. 43. A representação numérica da criticidade de um Ativo de TI do COMAER será calculada a partir do Nível de Gravidade Urgência e Tendência (GUT), conforme disposto na DCA 16/2 “Gestão de Riscos no Comando da Aeronáutica” ou normativo que vier a substituí-lo.

Art. 44. Os Elos do STI deverão manter um controle com os valores de criticidade dos ativos de TI em seu escopo de atuação, podendo agrupá-los por categorias.

CAPÍTULO VII
CLASSIFICAÇÃO DE NÍVEL DE ACESSO DAS INFORMAÇÕES

Art. 45. Todos os ativos de informação devem ser classificados de acordo com seu nível de acesso, a fim de assegurar o direito fundamental de acesso à informação, bem como dispor sobre a devida restrição de acesso sobre informações sigilosas, conforme previsto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI) e demais normas aplicáveis.

Art. 46. As informações armazenadas, transmitidas, processadas ou que se encontram sob a guarda dos ativos de informação da Organização, independentemente de seu formato e suporte, devem ser classificadas segundo seu nível de acesso, de acordo com a legislação pertinente, sobretudo com as disposições da LAI, do Decreto nº 7.724, de 16 de maio de 2012, e orientações ou normas complementares editadas por órgãos competentes.

Art. 47. A classificação de nível de acesso das informações deve observar às diretrizes constantes na LAI, Decreto nº 7.724, de 16 de maio de 2012 e outros normativos complementares que abordam o assunto.

Art. 48. As informações devem ser classificadas conforme os seguintes níveis de acesso:

I - pública - com acesso irrestrito e visível a todos os usuários, inclusive pelo público externo;

II - restrita - quando se tratar de informação sigilosa não classificada em grau de sigilo, protegidas por demais hipóteses legais de restrição de acesso; e

III - sigilosa - classificada em grau de sigilo, nos termos do art. 23 da lei nº 12.527/2011, subdividida nos graus ultrassecreto, secreto ou reservado.

Art. 49. Os ativos de informação serão rotulados e manuseados com base nos procedimentos apropriados de classificação de nível de acesso de informações usados pelo COMAER.

CAPÍTULO VIII
MANIPULAÇÃO DE MÍDIA

Art. 50. A mídia removível também deve ser gerenciada pelo mesmo procedimento de classificação de ativos de informação usado pelo COMAER.

Art. 51. A mídia removível deve ser protegida contra acesso não autorizado e uso indevido durante o uso e em trânsito, e deve ser descartada com segurança, usando os procedimentos para o desfazimento de bens de TI aprovados pelo Órgão Central do STI.

Art. 52. As mídias contendo informações confidenciais e internas das Organizações do COMAER devem ser protegidas contra acesso não autorizado, uso indevido, corrupção durante o transporte e, preferencialmente, com o uso de criptografia.

CAPÍTULO IX
USO ACEITÁVEL

Art. 53. Padrões ou diretrizes para o uso aceitável de ativos devem ser documentados para indicar o que os usuários dos ativos de informação podem ou não fazer.

Art. 54. Os seguintes itens devem ser cobertos nas diretrizes de uso aceitáveis:

I - uso do computador e dos sistemas de informação;

II - uso de **softwares** e dados;

III - uso da Internet e **e-mail**;

IV - uso do telefone; e

V - uso de equipamentos e materiais de escritório.

Art. 55. Os usos aceitáveis serão conforme o disposto na Política de Uso de Recursos Computacionais (Anexo II).

Art. 56. Como requisito de acesso ao ativo de informação e como componente do treinamento de conscientização de segurança, todos os usuários dos ativos de informação, sejam funcionários ou terceiros, serão obrigados a fornecer aceitação assinada das diretrizes de uso aceitáveis

ANEXO XV
POLÍTICA DE GESTÃO DE DADOS

Art. 1º O processo de gestão de dados no COMAER deve observar os seguintes parâmetros:

I - sensibilidade dos dados - todos os dados devem ser classificados de acordo com seu nível de sensibilidade, sendo essas classificações: reservado, secreto, ultrassecreto, conforme legislação vigente. A classificação deve ser revisada periodicamente para garantir sua precisão e adequação; e

II - proprietário dos dados - cada dado deve ter um proprietário formalmente designado, que será responsável por sua proteção e gestão ao longo de seu ciclo de vida. O proprietário deverá garantir o cumprimento das políticas de segurança da informação, definir controles de acesso, e assegurar a conformidade com as legislações em vigor;

III - manuseio dos dados - o manuseio dos dados deve seguir diretrizes rigorosas de segurança, incluindo a criptografia de dados sensíveis durante seu transporte e armazenamento. Acesso e manipulação devem ser restritos e baseados em controle de acesso por função, minimizando a exposição e garantindo auditabilidade.

IV - retenção dos dados - os dados devem ser retidos conforme os prazos estabelecidos por esta a Política de Gestão de Registros (**Logs**) de Auditoria – PGRA , respeitando as regulamentações legais vigentes;

V - requisitos de descarte - o descarte de dados deve ser realizado de forma segura, utilizando técnicas de “apagamento seguro” e destruição física de mídias. Deve ser garantido que dados sensíveis ou pessoais não possam ser recuperados após o descarte:

Art. 2º O Controle de Acesso Baseado em Funções (RBAC) deve ser implementado de forma padronizada em todos os sistemas de dados, com observância aos seguintes requisitos:

a) estabelecer permissões e privilégios para cada função, garantindo o acesso necessário sem excessos;

b) revisar, regularmente, o mapeamento de privilégios a fim de manter sua atualização;

c) automatizar o processo de concessão e revogação de acesso sempre que possível;

d) integrar a atribuição de acesso com o sistema de autenticação;

e) garantir a separação de funções críticas para evitar conflitos de interesse;

f) revisar o inventário de funções anualmente;

g) monitorar acessos anômalos ou não conformes com as políticas organizacionais; e

h) revogar automaticamente os privilégios de usuários que mudam de função ou deixam a organização.

Art. 3º O Órgão Central do STI poderá solicitar que os Elos Especializados do STI realizem auditorias, periodicamente, para assegurar a conformidade com esta Política e com os regulamentos de segurança da informação aplicáveis.

Parágrafo único. Essas auditorias deverão verificar o cumprimento das diretrizes estabelecidas para a retenção, manuseio e descarte de dados, além de identificar potenciais vulnerabilidades ou não conformidades que possam comprometer a segurança dos dados.

Art. 4º Os Elos do STI deverão providenciar que os militares e colaboradores responsáveis pela área de Gestão de Dados sejam capacitados na área.

Parágrafo único. A capacitação deverá abranger aspectos técnicos e legais, conforme exigido pela LGPD e outras regulamentações aplicáveis, garantindo que os envolvidos estejam aptos a cumprir as normas e boas práticas de segurança da informação.

ANEXO XVI
POLÍTICA DE CONTROLE DE ACESSO

CAPÍTULO I
PROPÓSITO

Art. 1º Esta Política de Controle de Acesso estabelece controles de identificação, autenticação e autorização para salvaguardar as informações do COMAER, estejam elas em qualquer meio, seja digital ou físico, a fim de evitar a quebra da segurança da informação e quaisquer acessos não autorizados que implique em risco de destruição, alteração, perda, roubo ou divulgação indevida.

Art. 2º Sem controles de autorização, identificação e autenticação, existe o risco potencial de que os sistemas de informação possam ser acessados ilicitamente e que a segurança desses sistemas de informação seja comprometida.

Art. 3º Considera-se, portanto, que as credenciais: crachá de identificação funcional e logins de acesso dos sistemas de informações, são pessoais e intransferíveis e são o único método legítimo pelo qual o direito de acesso físico e/ou lógico podem ser exercidos.

Art. 4º Os controles de autorização, identificação e autenticação garantem que apenas usuários autorizados tenham acesso físico ou façam uso dos sistemas de informação do COMAER.

CAPÍTULO II
ESCOPO

Art. 5º Esta Política se aplica a todas as informações, cujo COMAER seja o agente de tratamento, ao meio utilizado para este tratamento, seja digital ou físico, e as dependências físicas desta organização, bem como a qualquer pessoa que circule nas dependências ou que interaja exercendo controle administrativo, técnico ou operacional, mesmo que eventual, desses meios de tratamento.

Art. 6º Especificamente, inclui:

I - todos os funcionários, sejam servidores efetivos ou temporários, do COMAER;

II - todos os contratados e terceiros que trabalham para o COMAER; e

III - todos os funcionários de parceiros que acessam fisicamente as dependências ou que acessam a rede e sistemas de informação do COMAER.

CAPÍTULO III
DECLARAÇÕES DA POLÍTICA

Seção I
Dos princípios gerais:

Art. 7º A Política de Gestão de Controle de Acesso deve permanecer alinhada com a Política de Segurança da Informação do COMAER.

Art. 8º A Política de Gestão de Controle de Acesso deve permanecer alinhada com uma gestão de continuidade de negócios em nível organizacional.

CAPÍTULO IV
ACESSO LÓGICO

Art. 9º O acesso lógico aos recursos da Rede Local deve ser realizado por meio de sistema de controle de acesso. O acesso deve ser concedido e mantido pelos Elos do STI, em seu escopo de atuação, baseado nas responsabilidades e tarefas de cada usuário:

I - os Elos do STI devem implementar protocolos de comunicação e redes seguros;

II - terão direito a acesso lógico aos recursos da Rede Local os usuários de recursos de tecnologia da informação;

III - o acesso remoto deve ser realizado por meio de VPN (Rede Virtual Privada), após as devidas autorizações, conforme ato normativo específico do STI;

IV - deve ser utilizado o MFA para a autenticação de acesso remoto;

V - o acesso a todas as aplicações corporativas ou de terceiros que estejam hospedados em fornecedores deve utilizar MFA;

VI - o STI deve centralizar a autenticação, autorização e auditoria (AAA) dos ativos de informação da infraestrutura de rede do COMAER; e

VII - o STI deve adotar técnicas de segmentação de rede visando limitar o acesso de forma eficiente e segura, assegurando que apenas colaboradores e dispositivos autorizados possam interagir com partes específicas da rede.

Art. 10. Os Elos do STI, devem estabelecer e manter um inventário de todas as contas gerenciadas, este deve incluir contas de usuário, administrativas, testes e serviço. Em caso de contas de serviço, o inventário deve conter no mínimo informações de:

I - setor proprietário; e

II - data de criação/última autorização de renovação de acesso.

Parágrafo único. Compete ao Elo do STI responsável pela gestão dos acessos a validação de todas as contas ativas do órgão, a cada 90 (noventa), dias.

Art. 11. Os Elos do STI devem implementar a centralização da gestão de contas por meio de serviço de diretório e/ou identidade em seu escopo de atuação.

Art. 12. Os Elos do STI devem estabelecer e manter um inventário dos sistemas de autenticação e autorização da organização, tal inventário deve ser revisado periodicamente.

Art. 13. Os Elos do STI devem centralizar o controle de acesso para todos os ativos de informação em seu escopo de atuação por meio de um serviço de diretório ou provedor de SSO.

Art. 14. Os Elos do STI responsáveis por gestão dos acessos devem definir e manter o controle de acesso dos usuários baseado em funções.

§ 1º Deve ser elaborada a documentação dos direitos dos acessos para cada função dentro da organização.

§ 2º Compete aos Elos do STI responsáveis por gestão dos acessos a realização de análises de controle de acesso aos ativos institucionais para validar se todos os privilégios estão autorizados para a execução de atividades de cada função, este processo deve ser repetido de forma periódica ou quando novas funções e ativos de informação forem inseridos na organização; e

§ 3º Ao conceder acesso a usuários que lidam com dados pessoais, deve-se limitar, estritamente, o acesso aos sistemas que processam esses dados ao mínimo necessário para cumprir os objetivos essenciais do processamento, em conformidade com o princípio da minimização de dados. Ao atribuir ou revogar os direitos de acesso concedidos deve-se incluir:

I - verificação de que o nível de acesso concedido é apropriado às políticas de acesso, além de ser consistente com outros requisitos, tais como, segregação de funções;

II - garantia de que os direitos de acesso não estão ativados antes que o procedimento de autorização esteja completo;

III - manutenção de um registro preciso e atualizado dos perfis dos usuários criados para os que tenham sido autorizados a acessar o sistema de informação e os dados pessoais neles contidos;

IV - mudança dos direitos de acesso dos usuários que tenham mudado de função ou de atividades, e imediata remoção ou bloqueio dos direitos de acesso dos usuários que deixaram o COMAER; e

V - analisar criticamente os direitos de acesso em intervalos regulares.

Art. 15. Os Elos do STI responsáveis por gestão dos acessos devem implementar um processo formal de registro de usuários que tratem de dados pessoais para permitir atribuição de direitos de acesso e fornecer medidas para lidar com o comprometimento do controle de acesso do usuário, como corrupção ou comprometimento de senhas ou outros dados de registro do usuário, para tanto podem ser realizadas as seguintes ações:

I - o uso de um identificador de usuário único, para permitir relacionar os usuários com suas responsabilidades e ações;

II - o uso compartilhado de identificador de usuário somente será permitido, onde eles são necessários por razões operacionais ou de negócios e deverá ser aprovado e documentado; e

III - a garantia de que o um mesmo identificador de usuário não é emitido para outros.

CAPÍTULO V
CONTA DE ACESSO LÓGICO E SENHA

Art. 16. Para utilização das estações de trabalho do COMAER, será obrigatório o uso de uma única identificação (**login**) e de senha de acesso, fornecidos pelo STI, mediante abertura de chamado SAU pelo setor de pessoal da unidade do requisitante.

I - o Elo de Serviço do STI criará o perfil de acesso do usuário com base na função informada no chamado SAU, após o recebimento do Termo de Responsabilidade da Política de Controle de Acesso (Anexo XXVI), preenchido e assinado;

II - os privilégios de acesso dos usuários à Rede Local devem ser definidos pela unidade requisitante ao qual o usuário está vinculado, limitando-se a atividades estritamente necessárias à realização de suas tarefas; e

III - na necessidade de utilização de perfil diferente do disponibilizado, o setor de pessoal da unidade do usuário deverá solicitar via chamado SAU ao Elo do STI responsável pela gestão de acessos que a examinará, podendo negá-la nos casos em que a entender desnecessária.

Art. 17. O **login** e senha são de uso pessoal e intransferível, sendo proibida a sua divulgação, sob pena de serem bloqueados pelo Elo do STI responsável pela gestão de acessos quando constatada qualquer irregularidade.

Parágrafo único. Para retomar o acesso à rede, deverá ser formalizada uma requisição pelo titular da unidade do requisitante.

Art. 18. O padrão adotado para o formato da conta de acesso do usuário é uma sequência de letras minúsculas que identifiquem o nome-de-guerra do militar (quando civil, será utilizado o nome pelo qual é conhecido o funcionário) seguido das iniciais do nome.

Parágrafo único. Nos casos de já existência de conta de acesso para outro usuário, o Elo do STI responsável pela gestão de acessos acrescentará um numeral representando a repetição logo após as iniciais da pessoa.

Art. 19. O padrão adotado para o formato da senha deve considerar o tamanho mínimo de caracteres, a tipologia (letras, número e símbolos) e a proibição de repetição de senhas anteriores.

§ 1º a formação da senha da identificação (**login**) de acesso à Rede Local deve seguir as regras de:

a) possuir tamanho mínimo de oito caracteres, sendo obrigatório o uso de letras e números, para contas que utilizam MFA e 14 caracteres para contas que não utilizam MFA;

b) recomenda-se a utilização de letras maiúsculas, minúsculas e caracteres especiais ($, %, &,...);

c) não ser formada por sequência numérica (123...), alfabética (abc...), nomes próprios, palavras de fácil dedução, datas, placa de carro, número de telefone, a própria conta de acesso, apelidos ou abreviações;

d) não utilizar termos óbvios, tais como: Brasil, senha, usuário, **password** ou **system**; e

e) não reutilizar as últimas 05 (cinco) senhas.

§ 2º Os Elos do STI responsáveis pela gestão de acessos fornecerão uma senha temporária para cada conta de acesso criada no momento da liberação dessa conta e a mesma deverá ser alterada pelo usuário quando do primeiro acesso à Rede Local.

Art. 20. As senhas de acesso serão renovadas a cada 90 (noventa) dias, devendo o usuário ser informado antecipadamente a fim de que ele próprio efetue a mudança.

Parágrafo único. Caso não efetue a troca no prazo estabelecido, será bloqueado seu acesso à Rede Local até que a nova senha seja configurada.

CAPÍTULO VI
BLOQUEIO, DESBLOQUEIO E CANCELAMENTO DA CONTA DE ACESSO

Art. 21. A conta de acesso será bloqueada nos seguintes casos:

I - após 3 (três) tentativas consecutivas de acesso errado;

II - solicitação do superior imediato do usuário com a devida justificativa;

III - quando da suspeita de mau uso dos serviços disponibilizados pelo STI ou descumprimento da Política de Segurança da Informação e normas correlatas em vigência; e

IV - após 45 (quarenta e cinco) dias consecutivos sem movimentação pelo usuário.

Art. 22. O desbloqueio da conta de acesso à Rede Local será realizado apenas após solicitação formal do superior imediato do usuário ao Elo do STI responsável pela gestão de acessos.

Art. 23. Quando do afastamento temporário do usuário, a conta de acesso deve ser bloqueada a pedido do superior imediato ou do Setor responsável pela Gestão de Pessoas da OM.

Art. 24. A conta de acesso não utilizada há mais de 180 (cento e oitenta) dias poderá ser cancelada.

Art. 25. Os Elos do STI responsáveis pela gestão de acessos devem garantir a implementação de um processo formal de cancelamento de usuários que administrem ou operem sistemas e serviços que tratem de dados pessoais. Tal processo deverá incluir:

I - a imediata remoção ou desabilitação de usuário que tenha deixado a OM;

II - a remoção e identificação, de forma periódica, ou a desabilitação de usuários com os mesmos identificadores.

Art. 26. Os Elos do STI responsáveis pela gestão de acessos devem configurar o bloqueio automático de sessão nos ativos após um período de inatividade preestabelecido. Tal prazo pode ser específico para cada tipo de ativo.

Art. 27. Os Elos do STI responsáveis pela gestão de acessos devem, sempre que possível, priorizar a revogação/desativação de contas com o objetivo de manter dados e **logs** para possíveis auditorias.

CAPÍTULO VII
ACESSO FÍSICO

Art. 28. As OM do COMAER devem definir perímetros de segurança para proteger ambientes e ativos contra acesso físico não autorizado, danos e interferências de acordo com as diretrizes a seguir:

I - definir a localização e resistência dos perímetros de acordo com os requisitos de segurança da informação relacionados aos ativos que se encontre dentro dos perímetros;

II - proteger os ambientes seguros contra acessos não autorizados por meio de mecanismos de controle de acesso, como fechaduras tradicionais ou digitais, que possibilitem autenticação por biometria, senhas, PINS ou cartões de acesso; e

a) as OM do COMAER devem executar testes nos mecanismos de controle de acesso em períodos pré-definidos para assegurar a funcionalidade total do equipamento; e

b) os mecanismos de controle de acesso devem ser monitorados pelos Elos do STI responsáveis por monitoração.

III - estabelecer uma área de recepção ou outros meios de controle de acesso físico a ambientes que não for conveniente a implementação de mecanismos de controle de acesso.

Art. 29. O acesso físico a ambientes seguros ou ativos de tratamento e armazenamento de dados das OM do COMAER é destinado apenas a pessoal autorizado.

Art. 30. As OM do COMAER devem manter um processo de gestão de acessos para fornecimento, revisão periódica, atualização e revogação das autorizações.

Art. 31. As OM do COMAER devem implementar e manter seguro **logs** ou registro físico de todos os acessos aos ativos de informação.

Art. 32. O acesso a ambientes seguros ou ativos de tratamento e armazenamento de dados por fornecedores ou prestadores de serviços será concedido somente quando necessário e de acordo com as seguintes diretrizes:

I - para fins específicos e autorizados;

II - autorização concedida pelo Elo do STI responsável pela gestão de acesso ou pelo responsável pelo ativo; e

III - supervisionado e monitorado;

Art. 33. Os ativos de armazenamento e tratamento de dados que se encontrem fora do COMAER devem ser protegidos contra perda, roubos, danos e acesso físico não autorizados conforme as seguintes diretrizes:

I - não deixar o ativo sem vigilância em locais públicos e inseguros;

II - proteger o ativo contra riscos associados a visualização de informações por outra pessoa;

III - implementar as funcionalidades de rastreamento e limpeza remota.

Art. 34. O STI estabelecerá uma política ou normativo equivalente sobre a gestão de mídias de armazenamento, de acordo com as seguintes diretrizes:

I - exigir autorização para a saída de mídias de armazenamento do COMAER;

II - armazenar mídias em local seguro de acordo com a classificação de suas informações;

III - criptografar as mídias de acordo com a classificação de suas informações; e

IV - manter cópias de segurança de mídias de acordo com a classificação de suas informações;

Art. 35. O STI deve elaborar uma política ou normativo equivalente que defina condições e restrições pertinentes ao acesso físico nos dispositivos de trabalho remoto, levando em consideração as seguintes diretrizes:

I - segurança física do local de trabalho remoto;

II - regras e orientações quanto ao acesso de familiares e visitantes ao dispositivo.

CAPÍTULO VIII
MOVIMENTAÇÃO INTERNA

Art. 36. Quando houver mudança do usuário para outro setor ou o usuário ocupar uma nova função, os direitos de acesso à Rede Local devem ser revogados:

I - o novo superior imediato ou o Setor responsável pela Gestão de Pessoas da OM deve realizar a solicitação de novos acessos de acordo com novo setor / função do usuário.

II - os direitos de acesso antigos devem ser imediatamente cancelados conforme solicitação do antigo superior imediato ou do Setor responsável pela Gestão de Pessoas da OM.

CAPÍTULO IX
CONTA DE ACESSO BIOMÉTRICO

Art. 37. A conta de acesso biométrico, quando implementada, deve ser vinculada a uma conta de acesso lógico e ambas devem ser utilizadas para se obter um acesso, a fim de atender os conceitos da autenticação de multifatores.

Parágrafo único. O COMAER deverá tratar seus respectivos dados biométricos como dados sigilosos, preferencialmente, utilizando-se de criptografia, na forma da legislação vigente.

CAPÍTULO X
ADMINISTRADORES

Art. 38. A utilização de identificação (**login**) com acesso no perfil de administrador é permitida somente para usuários cadastrados para execução de tarefas específicas na administração de ativos de informação:

I - somente os técnicos dos Elos do STI, devidamente identificados e habilitados, terão senha com privilégio de administrador nos equipamentos locais e na rede;

II - na necessidade de utilização de **login** com privilégio de administrador do equipamento local, o usuário deverá encaminhar solicitação para o Elo do STI responsável pela gestão dos acessos, que poderá negar os casos em que entender desnecessária a utilização;

III - se concedida a permissão ao usuário como administrador local na estação de trabalho, esse será responsável por manter a integridade da máquina, não podendo instalar, desinstalar ou remover qualquer programa sem autorização formal do Elo do STI responsável pelos serviços de TI da OM;

IV - caso constatada a irregularidade, o usuário perderá o acesso como administrador, não mais podendo requerer outra permissão;

V - a identificação (**login**) com privilégio de administrador nos equipamentos locais será fornecida em caráter provisório, podendo ser renovada por solicitação formal do titular da unidade requisitante;

VI - salvo para atividades específicas da área responsável pela gestão da tecnologia da informação do órgão, não será concedida, para um mesmo usuário, identificação (login) com privilégio de administrador para mais de uma estação de trabalho, ou para acesso a equipamentos servidores e a dispositivos de rede;

VII - excepcionalmente, poderão ser concedidas identificações (*login*) de acesso à rede de comunicação de dados a visitante em caráter temporário após apreciação do Comandante da OM por meio do Elo do STI responsável pela gestão dos acessos;

VIII - os Elo do STI responsáveis pela gestão dos acessos devem implementar o MFA para todas as contas de administrador;

IX - os Elo do STI responsáveis pela gestão dos acessos devem restringir os privilégios de administrador a contas de administrador dedicados nos ativos de informação, para que o usuário com privilégio de administrador não consiga realizar atividades gerais de computação, como navegação na Internet, **e-mail** e uso do pacote de produtividade, estas atividades deverão ser realizadas preferencialmente a partir da conta primária não privilegiada do usuário; e

X - ao tratar dados pessoais as OM do COMAER devem observar o princípio do privilégio

mínimo como regra, para garantir que o usuário receba apenas os direitos mínimos necessários para executar suas atividades, para tanto podem ser realizadas as seguintes ações por meio dos Elos do STI responsáveis pela gestão de ativos:

a) remover os direitos de administrador nos dispositivos finais;

b) remover todos os direitos de acesso root e admin aos servidores e utilizar tecnologias que permitam a elevação granular de privilégios conforme a necessidade, ao mesmo tempo em que fornecem recursos claros de auditoria e monitoramento;

c) eliminar privilégios permanentes (privilégios que estão "sempre ativos") sempre que possível;

d) limitar a associação de uma conta privilegiada ao menor número possível de pessoas; e

e) minimizar o número de direitos para cada conta privilegiada.

CAPÍTULO XI
RESPONSABILIDADES

Art. 39. É de responsabilidade do superior imediato do usuário comunicar formalmente ao Setor responsável pela Gestão de Pessoas da OM e ao Elo do STI responsável pela gestão dos acessos o desligamento ou saída do usuário da OM para que as permissões de acesso à Rede Local sejam canceladas.

Art. 40. Caberá ao Setor responsável pela Gestão de Pessoas das OM do COMAER a comunicação imediata ao Elo do STI responsável pela gestão dos acessos sobre desligamentos, férias e licenças de servidores e estagiários, para que seja efetuado o bloqueio momentâneo ou a revogação definitiva da permissão de acesso aos recursos.

Art. 41. Compete aos setores responsáveis pela gestão de mão-de-obra terceirizada nas OM do COMAER a comunicação imediata ao Elo do STI responsável pela gestão dos acessos da Informação sobre desligamentos, férias e licenças de funcionários de empresas prestadoras de serviços, para que seja efetuado o bloqueio momentâneo ou revogação definitiva da permissão de acesso aos recursos:

I - os serviços serão filtrados por programas de **antivírus**, **anti-phishing** e **anti-spam** e, caso violem alguma regra de configuração, serão bloqueados ou excluídos automaticamente; e

II - nenhum técnico do COMAER terá acesso ao conteúdo das informações armazenadas nos equipamentos servidores do COMAER.

Art. 42. Compete aos Elo do STI responsável pelos serviços de Tecnologia da Informação das OM o monitoramento da utilização de serviços de rede e de acesso à Internet, podendo ainda exercer fiscalização nos casos de apuração de uso indevido desses recursos, bem como bloquear, temporariamente, sem aviso prévio, a estação de trabalho que esteja realizando atividade que coloque em risco a segurança da rede, até que seja verificada a situação e descartada qualquer hipótese de dano à infraestrutura tecnológica do COMAER.

Art. 43. O usuário é responsável por todos os acessos realizados através de sua conta de acesso e por possíveis danos causados à Rede Local e a recursos de tecnologia custodiados ou de propriedade do COMAER:

I - o usuário é responsável pela integridade e utilização de sua estação de trabalho, devendo, no caso de sua ausência temporária do local onde se encontra o equipamento, bloqueá-lo ou desconectar-se da estação, para coibir acessos indevidos;

II - a utilização simultânea da conta de acesso à Rede Local em mais de uma estação de trabalho ou notebook deve ser evitada, sendo responsabilidade do usuário titular da conta de acesso os riscos que a utilização paralela implica; e

III - o usuário não poderá, em hipótese alguma, transferir ou compartilhar com outrem sua conta de acesso e respectiva senha à Rede Local.

Art. 44. O usuário deve informar ao Elo do STI responsável pelos serviços de Tecnologia da Informação qualquer situação da qual tenha conhecimento que configure violação de sigilo ou que possa colocar em risco a segurança inclusive de terceiros.

Art. 45. É dever de o usuário zelar pelo uso dos sistemas informatizados, tomando as medidas necessárias para restringir ou eliminar riscos para a Instituição, a saber:

I - não permitir a interferência externa caracterizada como invasão, monitoramento ou utilização de sistemas por terceiros, e outras formas;

II - evitar sobrecarga de redes, de dispositivos de armazenamento de dados ou de outros, para não gerar indisponibilidade de informações internas e externas;

III - interromper a conexão aos sistemas e adotar medidas que bloqueiem o acesso de terceiros, sempre que completarem suas atividades ou quando se ausentarem do local de trabalho por qualquer motivo;

IV - não se conectar a sistemas e não buscar acesso a informações para as quais não lhe tenham sido dadas senhas e/ou autorização de acesso;

V - não divulgar a terceiros ou a outros usuários dispositivos ou programas de segurança existentes em seus equipamentos ou sistemas;

VI - utilizar corretamente os equipamentos de informática e conservá-los conforme os cuidados e medidas preventivas estabelecidas;

VII - não divulgar suas senhas e nem permitir que terceiros tomem conhecimento delas, reconhecendo-as como pessoais e intransferíveis; e

VIII - assinar o Termo de Responsabilidade da Política de Controle de Acesso (Anexo XXVI), quanto a utilização da respectiva conta de acesso.

CAPÍTULO XII
DISPOSIÇÕES GERAIS

Art. 46. Os incidentes que afetem a Segurança das Informações, assim como o descumprimento da Política de Segurança da Informação e Normas de Segurança devem ser obrigatoriamente comunicados pelos usuários ao Elo do STI responsável pelos serviços de Tecnologia da Informação.

Art. 47. Quando houver suspeita de quebra da segurança da informação que exponha ao risco os serviços ou recursos de tecnologia, o Elo do STI responsável pelos serviços de Tecnologia da Informação fará a investigação, podendo interromper temporariamente o serviço afetado, sem prévia autorização.

I - nos casos em que o ator da quebra de segurança for um usuário, o Elo do STI responsável pelos serviços de Tecnologia da Informação comunicará o Elo Especializado responsável pela Segurança da Informação e ao seu superior imediato para adoção de medidas cabíveis;

II - ações que violem os controles de Segurança da Informação serão passíveis de sansões civis, penais e administrativas, conforme a legislação em vigor, que podem ser aplicadas isoladamente ou cumulativamente;

III - processo administrativo disciplinar específico deverá ser instaurado para apurar as ações que constituem em quebra das diretrizes impostas por esta política; e

IV - a resolução de casos de violação/transgressões omissos nas legislações correlatas será resolvida pelo Comitê de Governança Digital, de Segurança da Informação e de Proteção de Dados (CGDSIPD) do COMAER.

ANEXO XVII
POLÍTICA DE GESTÃO DE REGISTROS (LOGS) DE AUDITORIA – PGRA

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo da Política de Gestão de Registros (**Logs**) de Auditoria é estabelecer e manter um processo de gestão de **log** de auditoria que defina os requisitos de **log** no COMAER. Tal processo deve tratar da coleta, armazenamento, uso e exclusão de **logs** de auditoria e sistemas para os ativos de informação do COMAER. É importante que seja estabelecida a revisão periódica deste processo de gestão de **log** de auditoria.

CAPÍTULO II
ESCOPO

Art. 2º Esta Política de Gestão de Registros (**Logs**) de Auditoria (PGRA) se aplica aos ativos informacionais do COMAER, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e ou os utilize, com responsabilidades específicas a indivíduos atuantes na gestão, processo e desenvolvimento em nome COMAER.

Parágrafo único. Essa política também se aplica, nos limites estabelecidos contratualmente, a quaisquer provedores e entidades terceirizadas com acesso aos ativos de informação o COMAER.

Art. 3º Podem ocorrer de alguns ativos de informação COMAER não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas.

Art. 4º Quaisquer exceções a esta política deverão ser documentadas submetidas à aprovação do Órgão Central do STI.

Parágrafo único. Tais exceções devem ser tratadas no mapeamento de riscos de segurança da informação do COMAER, conforme disposto no Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

CAPÍTULO III
PREMISSAS E RESPONSABILIDADES

Art. 5º A atividade de auditoria no COMAER é de competência de equipe técnica designada pelo Elo Especializado do STI designado como responsável pela Gestão de Registros de Auditoria, devendo este se reportar ao Órgão Central do STI.

§ 1º O Elo Especializado deve assegurar que a equipe responsável possua capacidade técnica e experiência nas áreas de gerenciamento de logs, disponha de competências técnico-administrativas necessárias ao bom desempenho de suas funções, quais sejam: independência, autonomia, imparcialidade, zelo, integridade e ética profissional, além de autoridade para avaliar as funções próprias e as funções terceirizadas no âmbito do COMAER.

§ 2º A equipe responsável pela auditoria pode obter assessoria de especialistas/consultores externos ou mesmo equipe terceirizada para subsidiar a área quando essa não for suficientemente proficiente.

§ 3º A equipe responsável pela auditoria, quando executa a atividade de auditoria, deve possuir acesso irrestrito às informações necessárias ao bom desempenho de suas funções, quais sejam: acesso irrestrito a quaisquer informações, ambientes e ativos de informação.

§ 4º É dever dos Elos do STI cooperar com a equipe responsável pela auditoria quanto ao acesso a ativos de informação, instalações e trânsito de dados.

§ 5º Os membros da equipe responsável pela auditoria devem ter canal de comunicação permanente com os demais Elos do STI, para apoiar na atuação corretiva, de forma apropriada e tempestiva, em resposta às recomendações decorrentes dos trabalhos de auditoria.

Art. 6º Os eventos de **log** devem ser gerados, selecionados e armazenados para todos os ativos.

Art. 7º A equipe responsável pela auditoria deve selecionar os eventos e os respectivos tempos de guarda, bem como as demais características de uso dos eventos.

Art. 8º As exceções deverão ser documentadas e comunicadas ao Órgão Central do STI.

CAPÍTULO IV
REQUISITOS DO PLANO DE REGISTROS DE AUDITORIA

Art. 9º Os Elos do STI devem habilitar, em seu escopo de atuação, a coleta de registro de logs em cada um dos dispositivos existentes para a execução de tarefas, e deve fornecer recursos cibernéticos dedicados para armazenar todos os dados coletados.

Art. 10. Os recursos cibernéticos utilizados para armazenamento dos logs devem ser segmentados da rede primária e que não seja permitido o acesso a rede externa.

Art. 11. Ativos de informação devem ser configurados de forma a sincronizar data e hora via NTP. Pelo menos duas fontes de tempo (relógios de referência) devem estar configuradas, para garantir que o sistema continue funcionando mesmo se um deles falhar.

Art. 12. Deve-se utilizar o horário de Greenwich em sistemas hospedados em provedores de nuvem onde o fuso local pode ser diferente do fuso do provedor.

Art. 13. Processos, procedimentos e medidas técnicas devem ser definidos e implementados visando a proteção dos dados sensíveis ao longo de seu ciclo de vida.

Art. 14. Devem ser mapeados os ativos de informação que podem ter suas configurações de **log** mais detalhadas com informações como: ID de usuário de acesso, IP do **host**, data, hora e fuso horário, acessos de usuários privilegiados, e que por qualquer motivo, não possa apresentar dados detalhados.

Art. 15. O Elo de Serviço de TI, além de monitorar eventos relacionados aos ativos de informação, pode também registrar os seguintes eventos de segurança da informação:

I - utilização de usuários, perfis e grupos privilegiados;

II - acoplamento e desacoplamento de dispositivos de **hardware**, principalmente mídias removíveis;

III - inicialização, suspensão e reinicialização de serviços;

IV - criação, modificação e exclusão de grupos ou listas de grupos com acessos privilegiados;

V - atualização das regras da política de senhas de usuários;

VI - criação, acesso e modificação de arquivos de sistemas considerados críticos;

VII - qualquer evento realizado nos ativos de informação de segurança existentes; e

VIII - em caso de incidentes de segurança da informação, ou quaisquer outros eventos de segurança, o Elo Especializado deve coletar e preservar todos os registros de eventos citados anteriormente e as mídias de armazenamento dos ativos de informação afetados pelo evento.

Art. 16. Caso não seja possível cumprir as diretrizes apontadas, em razão do reestabelecimento dos sistemas e serviços afetadas de forma rápida, o Elo Especializado deve coletar e armazenar cópias dos registros e arquivos afetados pelo incidente de segurança como:

I - logs;

II - arquivos de sistema operacional;

III - configurações do sistema operacional; e

IV - demais arquivos e **logs** que foram necessários para reestabelecimento do serviço ou sistema.

Art. 17. O Elo Especializado deve manter a estrutura original de diretórios além dos "metadados" destes arquivos tais como: data, hora de criação e atualização e permissões.

Art. 18. Em caso de impossibilidade de preservar as evidências do evento de segurança, o Elo de Serviço de TI deve justificar em relatório, a falta destas evidências.

Art. 19. As ações para o reestabelecimento do serviço e sistema afetados pelo evento de segurança não devem impossibilitar a coleta, a preservação e disponibilidade das evidências de forma íntegra.

Art. 20. Devem ser promovidas ações para a preservação dos arquivos coletados.

CAPÍTULO V
FASES DA GESTÃO DE REGISTROS DE AUDITORIA

Art. 21. Segue o detalhamento das quatro fases do processo de gerenciamento de **logs** de auditoria, divididas em coleta, armazenamento, uso e exclusão.

Seção I
Da coleta

Art. 22. O Elo Especializado deve coletar informações de tráfego IP e monitorar todo fluxo de rede.

Art. 23. Em caso de incidente de segurança da informação, todo e qualquer material coletado deverá ser lacrado e custodiado pelo Elo Especializado, e este deve preencher um Termo de Custódia dos Ativos de Informação relacionados ao incidente de segurança.

§ 1º O material coletado ficará à disposição do Elo Especializado, que ficará responsável por sua destinação.

§ 2º O Órgão Central do STI definirá o modelo de Termo de Custódia dos Ativos de Informação em ato normativo específico.

Art. 24. A geração de **log** de auditoria deve estar habilitada nos ativos de informação, seguindo as diretrizes do processo de gestão de registros de auditoria do Órgão Central do STI.

Art. 25. **Logs** e registros de auditoria de ativos de informação devem ser criados e retidos na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 26. **Logs** devem ser coletados em um ou mais repositórios centrais.

Art. 27. Deve ser assegurado que ativos de informação classificados como críticos estejam registrando **logs** de auditoria.

Art. 28. Usuários e componentes dos ativos de informação devem ser monitorados continuamente em busca de comportamento anômalo ou suspeito.

Art. 29. Ativos de informação dos Elos do STI devem gerar registros de auditoria para eventos definidos. Esses eventos definidos incluem a identificação de eventos significativos relevantes para a segurança da informação que precisam ser auditados.

Art. 30. A lista de eventos auditáveis definidos deve ser revisada e atualizada periodicamente, pelo menos a cada 180 dias.

Art. 31. Devem ser registrados os eventos de:

I - tentativas de **logon** (do sistema ou domínio) bem-sucedidas e malsucedidas;

II - gerenciamento de contas de usuários;

III - acesso ao serviço de diretório;

IV - uso privilegiado;

V - acompanhamento de processos;

VI - sistema; e

VII - destruição de arquivo de **log** de auditoria.

Art. 32. Entradas de trilha de auditoria para componentes do sistema podem ser registradas de forma classificada e personalizada, contendo:

I - identificação do usuário;

II - tipo de evento;

III - data e horário;

IV - indicação de sucesso ou falha;

V - origem do evento; e

VI - a identidade ou o nome dos dados afetados, componentes do sistema ou recurso.

Art. 33. Ativos de informação que contêm dados sensíveis aos negócios da Organização devem possuir **log** de auditoria detalhado, incluindo, mas não se limitando, a elementos úteis que possam ajudar em uma eventual investigação forense, sendo eles:

I - origem do evento;

II - data e hora do evento;

III - nome de usuário; e

IV - endereços de origem e destino.

Art. 34. Os Elos STI devem, ao manter registros de eventos (**logs**), considerando o princípio de minimização de dados, gravar o acesso ao dado pessoal, incluindo as seguintes informações, mas não se limitando a:

I - identificação do usuário;

II - data e hora do acesso;

III - qual titular de dados pessoais foi acessado; e

IV - quais mudanças (se houver alguma) foram feitas (adições, modificações ou exclusões).

Seção II
Do armazenamento

Art. 35. O armazenamento de **logs** deve estar de acordo com o processo de gestão de **logs** do Orgão Central do STI.

Art. 36. No caso dos **logs** armazenados conterem dados pessoais, deve-se observar o previsto pelo art. 16 da LGPD a fim de avaliar se os **logs** devem ser eliminados ou conservados após o término do tratamento dos dados pessoais.

Art. 37. O armazenamento dos **logs** de ativos que contenham dados classificados deve obedecer aos critérios de segurança estabelecidos pela ICA 205-47 “Instrução para a Salvaguarda de Assuntos Sigilosos da Aeronáutica (ISAS)”, garantindo o nível de proteção adequado aos assuntos sigilosos do COMAER.

Art. 38. Registros de auditoria devem ser retidos por pelo menos 180 dias. Uma vez que o período mínimo de retenção tenha sido atingido, os Elos do STI podem continuar a reter registros de auditoria até que seja determinado que eles não sejam mais necessários para fins administrativos, legais, de auditoria ou outros fins operacionais.

Art. 39. Os registros de **log** de auditoria e outros **logs** de eventos de segurança devem ser revisados e retidos de maneira segura.

Art. 40. O Elo Especializado responsável pela Gestão de Registros de Auditorias deverá implementar, se possível, trilhas de auditoria automatizadas para todos os componentes do sistema para reconstruir os seguintes eventos:

I - todos os acessos de usuários individuais aos dados classificados como sensíveis;

II - todas as ações desempenhadas por qualquer pessoa com privilégios root ou administrativos;

III - acesso a todas as trilhas de auditoria;

IV - tentativas inválidas de acesso lógico;

V - uso e as alterações dos mecanismos de identificação e autenticação, a criação de novas contas, aumento de privilégios e demais alterações, adições ou exclusões de contas com privilégios **root** ou administrativos;

VI - inicialização, interrupção ou pausa dos registros de auditoria; e

VII - criação e exclusão de objetos a nível do sistema.

Art. 41. A capacidade de armazenamento dos **logs** deve ser constantemente verificada.

Art. 42. Registros de auditoria devem ser correlacionados quando houver mais de um repositório de **logs** ou coletados de várias fontes de **logs**.

Art. 43. Cópias de segurança (**backups**) de arquivos de trilhas de auditoria de **log** devem ser armazenados de forma segura, em mídia de difícil alteração.

Seção III
Do uso

Art. 44. A frequência, escopo e/ou profundidade da revisão, análise e relatório dos registros de auditoria devem ser ajustados para atender às necessidades do COMAER com base nas informações recebidas.

Art. 45. Análises de **logs** de auditoria devem ser realizadas pelo menos 120 dias para detectar anomalias ou eventos anormais que possam indicar uma ameaça potencial.

Art. 46. Processos, procedimentos e medidas técnicas devem ser definidas pelo Elo Especializado, implementados e avaliados para reporte de anomalias e falhas do sistema de monitoramento e notificação imediata ao responsável, caso confirmado.

Art. 47. Eventos relacionados à segurança nos aplicativos e na infraestrutura subjacente devem ser identificados e monitorados.

Art. 48. **Logs** e registros de auditoria de sistemas devem ser configurados e armazenados na medida necessária para permitir o monitoramento, análise, investigação e relatório de atividades ilegais ou não autorizadas.

Art. 49. Em casos de resposta a incidentes cibernéticos, a coleta de dados forenses deve ser utilizada nos sistemas afetados, garantindo a transferência e a proteção de tais dados.

Art. 50. Conteúdo que deverá constar em cada evento auditado:

I - data e hora do evento;

II - o componente do ativo de informação (por exemplo, componente de **software**, componente de **hardware**) onde ocorreu o evento;

III - tipo de evento;

IV - identidade do usuário/sujeito; e

V - resultado (sucesso ou fracasso) do evento.

Art. 51. Os componentes do sistema e a operação desses componentes devem ser monitorados em busca de anomalias que sejam indicativas de atos maliciosos, desastres naturais e erros que afetem a capacidade de Organizações do COMAER de atingir seus objetivos. As anomalias devem ser analisadas para determinar se representam eventos ou incidentes de segurança.

Art. 52. Quando apropriado, **logs** de auditoria de consultas DNS e URL em ativos de informação devem ser coletados.

Art. 53. As implementações de coleta de **logs** podem incluir a coleta de **logs** de auditoria de linhas de comando (CLI) tais como **PowerShell**, **BASH** e terminais administrativos remotos.

Art. 54. O comportamento dos ativos de informação deve ser analisado para detectar e mitigar a execução de comandos e scripts que possam indicar ações maliciosas.

Art. 55. Quando apropriado, **logs** do provedor de serviços devem ser coletados.

Art. 56. Quando suportado, convém que o acesso a sistemas críticos por terceiros seja monitorado quanto a atividades não autorizadas ou incomuns.

Art. 57. Processos de revisão, análise e relatórios de registros de auditoria devem ser correlacionados, para investigação e resposta a indicações de atividades ilegais, não autorizadas, suspeitas ou incomuns.

Seção IV
Da exclusão

Art. 58. Quando não forem mais necessários para requisitos legais, regulatórios ou de negócios do COMAER, os dados de **logs** devem ser removidos dos registros usando um método seguro aprovado.

Art. 59. Deve-se implementar medidas de salvaguarda para os **logs**, bem como controles específicos para registro das atividades dos administradores e operadores dos sistemas relacionados ao objeto, de forma que esses não tenham permissão de exclusão ou desativação dos registros (log) de suas próprias atividades.

Art. 60. A exclusão deve ser feita de modo a assegurar a irrecuperabilidade, destruindo inclusive as cópias, mídias digitais, impressos e discos rígidos:

I - mídias digitais, como fita, CD/DVD e unidades flash, devem ser trituradas;

II - discos rígidos devem ser apagados usando um padrão recomendado para destruição de dados ou destruídos fisicamente;

III - cópias dos dados em sistemas ativos e de **backup**, devem ser destruídos fisicamente ou devem utilizar um padrão recomendado para destruição; e

IV - cópias impressas dos **logs** e relatórios em papel devem ser cortadas em tiras (picotados) e incinerados.

Art. 61. No caso em que o descarte/exclusão for realizado por meio de terceiro, deve-se incluir registro/rastreamento quando enviado por correio seguro ou outro método de entrega.

Art. 62. Mídias digitais de armazenamento ou discos rígidos podem ser reutilizados, desde que seja realizada a sobrescrição de dados na mídia a ser reutilizada.

CAPÍTULO VI
RECOMENDAÇÕES TÉCNICAS

Art. 63. As equipes que atuam no processo de Gestão de Registros de Auditorias devem atentar para as seguintes recomendações técnicas:

I - restringir a instalação de aplicativos e **softwares** - o privilégio de instalação de aplicativos e **softwares** deve ser restrito a indivíduos autorizados obedecendo os critérios do órgão ou entidade.

II - desabilitar **logs** na nuvem - agentes mal-intencionados podem desabilitar recursos e

integrações de **log** na nuvem para limitar quais dados são coletados em suas atividades e evitar a detecção.

III - desabilitar a inicialização TFTP (**Trivial File Transfer Protocol**) - agentes mal-intencionados podem abusar da inicialização pela rede para carregar um sistema operacional de dispositivo de rede não autorizado a partir de um servidor TFTP. A inicialização TFTP (**netbooting**) é comumente usada por administradores de rede para carregar imagens de dispositivos de rede controladas por configuração de um servidor de gerenciamento centralizado. A inicialização por rede é uma opção na sequência de inicialização e pode ser usada para centralizar, gerenciar e controlar imagens de dispositivos.

IV - remover indicador no **host** – agentes mal-intencionados podem excluir ou alterar artefatos gerados em um sistema **host**, incluindo **logs** ou arquivos capturados, como **malware** em quarentena. Os locais e o formato dos **logs** são específicos da plataforma ou do produto, no entanto, os **logs** do sistema operacional padrão são capturados como eventos do **Windows** ou arquivos **Linux**/**macOS**, como **Bash History** e /var/log/*.

V - limpar **logs** de eventos do **Windows** – agentes mal-intencionados podem limpar os **logs** de eventos do **Windows** para ocultar a atividade de uma intrusão. Os **logs** de eventos do Windows são um registro de alertas e notificações de um computador. Existem três fontes de eventos definidas pelo sistema: sistema, aplicativo e segurança, com cinco tipos de eventos: erro, aviso, informações, auditoria de sucesso e auditoria de falha.

VI - limpar **logs** do sistema **Linux** ou **Mac** - agentes mal-intencionados podem limpar os **logs** do sistema para ocultar evidências de uma invasão. O **macOS** e o **Linux** acompanham as ações do sistema ou iniciadas pelo usuário por meio de **logs** do sistema. A maioria dos **logs** do sistema nativo é armazenada no diretório /var/log/. As subpastas neste diretório categorizam os **logs** por suas funções relacionadas, como:

a) **At (Linux)** - agentes mal-intencionados podem abusar do utilitário **at** para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O comando **at** nos sistemas operacionais **Linux** permite que os administradores programem tarefas;

b) **Launchd** - agentes mal-intencionados podem abusar do **daemon Launchd** para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O **daemon launchd**, nativo do **macOS**, é responsável por carregar e manter os serviços dentro do sistema operacional. Esse processo carrega os parâmetros para cada **daemon** de nível de sistema de inicialização sob demanda dos arquivos de lista de propriedades (**plist**) encontrados em /**System/Library/LaunchDaemons** e **/Library/LaunchDaemons**. Esses **LaunchDaemons** possuem arquivos de lista de propriedades que apontam para os executáveis que serão lançados; e

c) **Cron** - agentes mal-intencionados podem abusar do utilitário **cron** para realizar o agendamento de tarefas para execução inicial ou recorrente de código malicioso. O utilitário **cron** é um agendador de tarefas baseado em tempo para sistemas operacionais do tipo **Unix**. O arquivo **crontab** contém o agendamento das entradas **cron** a serem executadas e os tempos especificados para execução. Todos os arquivos **crontab** são armazenados em caminhos de arquivo específicos do sistema operacional.

CAPÍTULO VII
PROCEDIMENTOS RELEVANTES

Art. 64. Definições complementares sobre a Gestão de Registros (Logs) de Auditoria serão abordadas em ato normativo específico do STI.

ANEXO XVIII
POLÍTICA DE DEFESAS CONTRA MALWARE

CAPÍTULO I
PROPÓSITO

Art. 1º O objetivo desta política é garantir a proteção adequada contra **malware** em todos os ativos de informação e que os controles de proteção recomendados para estes ativos de informação estejam em vigor.

Art. 2º Em sua missão, o STI deve assegurar a segurança e a continuidade do negócio do COMAER por meio da adoção de defesas **antimalware** atualizadas e aplicadas em todos os pontos de entrada e ativos da instituição. Isso é essencial para identificar e impedir a disseminação ou gerenciar a execução de **softwares** ou códigos mal-intencionados.

Art. 3º Os ativos de informação do COMAER devem ser classificados a fim de permitir a definição de níveis de segurança para eles.

Parágrafo único. Deverá ser definido para cada ativo de informação um "proprietário", o qual realizará a classificação do ativo de informação, registrando-o em uma base de dados gerenciada de forma centralizada.

CAPÍTULO II
ESCOPO

Art. 4º Esta Política de Defesas Contra Malware se aplica a todos os processos de negócios e dados, sistemas de informação e componentes, pessoal e áreas físicas do COMAER.

Art. 5º Esta Política se aplica em todos os possíveis pontos de entrada e ativos institucionais para detectar e impedir a propagação ou controlar a execução de **software** ou código malicioso.

CAPÍTULO III
DOS PRINCÍPIOS GERAIS

Art. 6º A Política de Defesas contra Malware deve permanecer alinhada com a Política de Segurança da Informação do COMAER.

Art. 7º A PDM deve permanecer alinhada com uma gestão de continuidade de negócios em nível organizacional.

Art. 8º Esta Política apresenta um conjunto de diretrizes para lidar com os incidentes e eventos de **malware** que porventura possam ocorrer no âmbito institucional.

§ 1º Esta Política não anula a necessidade de tratar especificidades de cada tipo de **malware**.

§ 2º A depender do tipo de **malware**, pode-se considerar procedimentos diferentes para lidar com incidentes de cada categoria.

Art. 9º Os Elos do STI são responsáveis pela implementação desta Política em seu escopo de atuação.

Art. 10. Os Elos do STI devem empenhar-se em detectar e validar ameaças de **malware** rapidamente para minimizar o número de ativos de informação expostos e a quantidade de danos que possa vir a sofrer.

Art. 11. A PDM deve ser revisada e atualizada regularmente tanto para refletir as mudanças das ameaças e novas tecnologias quanto para garantir que esteja em conformidade com normas e regulamentações vigentes.

Art. 12. O Elo Especializado do STI responsável pelo CTIR.FAB devem ser avaliar continuamente a eficácia e efetividade da PDM, por meio de auditorias e análise de eventuais incidentes.

Art. 13. Os procedimentos para Gestão de Incidentes Cibernéticos no COMAER serão abordados em ato normativo específico.

CAPÍTULO IV
PAPÉIS E RESPONSABILIDADES

Art. 14. O Órgão Central e os Elos do STI devem garantir que todos os ativos de informação estejam de acordo com as diretrizes estabelecidas nesta Política.

Art. 15. Os Elos do STI devem documentar os procedimentos utilizados na atribuição de responsabilidades para lidar com a proteção nos ativos de informação e recuperação de ataques de **malware** em seu escopo de atuação.

CAPÍTULO V
CONSCIENTIZAÇÃO E TREINAMENTO

Art. 16. O Gestor de Segurança da Informação do COMAER, deve promover ações de conscientização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Art. 17. Os Elos de Serviço do STI devem promover a conscientização ou treinamento a todos os usuários sobre como identificar arquivos e programas infectados por **malware** e a quem relatar uma possível infecção.

Art. 18. O Órgão Central do STI deve basear-se em relatórios de eventos de **malware** ocorridos anteriormente para planejar o programa de conscientização e treinamento de seus colaboradores.

Art. 19. Criar e manter um programa de conscientização, educação e treinamento que aborde temas entendidos como importantes, levando em consideração a Política de Segurança da Informação e suas diretrizes.

Art. 20. O programa de conscientização e treinamento sobre **malware** do COMAER deve ser revisado e atualizado de forma periódica.

§ 1º O Elo Especializado do STI responsável pelo CTIR.FAB deve elaborar treinamentos específicos para os diferentes requisitos de segurança da informação inerentes a cada cargo ou função dos servidores do COMAER.

§ 2º O programa de conscientização e treinamento deve considerar o treinamento de novos colaboradores.

§ 3º O Órgão Central do STI deve criar e manter uma forma de avaliação do programa de conscientização e treinamento por meio de feedback dos participantes.

§ 4º O programa de conscientização e treinamento deve ter como um dos objetivos elucidar os colaboradores sobre as suas responsabilidades no que diz respeito a segurança da informação de ativos de informação do COMAER.

§ 5º O programa de conscientização do COMAER deve observar a importância de elaborar a conscientização e treinamento dos prestadores de serviço de acordo com novas contratações e encerramento de contrato.

§ 6º O programa de conscientização do COMAER pode utilizar de ferramentas como salas virtuais e físicas de treinamento, folhetos, cartazes, websites, boletins informativos e eventos específicos para manter o público-alvo, informado e atualizado sobre as diretrizes de proteção contra **malware** do COMAER.

§ 7º O COMAER deve conscientizar os seus colaboradores quanto a importância de relatar o mais rápido possível uma possível infecção ou evento de segurança da informação.

§ 8º O COMAER deve manter e divulgar de forma ampla o canal de comunicação de possíveis eventos de segurança da informação.

CAPÍTULO VI
PREVENÇÃO DE INCIDENTES DE MALWARE

Art. 21. O Órgão Central do STI deve adotar medidas que visam mitigar o impacto da exploração de vulnerabilidades por **malwares**, tais como a indisponibilidade de recursos (redes, aplicações e etc.) que venham a afetar negativamente a continuidade dos negócios do COMAER.

Art. 22. Os Elos do STI devem adotar técnicas de segmentação de rede visando mitigar a propagação ou disseminação de ameaças, tais como **malwares**, dentro da rede em seu escopo de atuação.

Art. 23. Os Elos do STI devem adotar, quando necessário, infraestrutura como código para a configuração e atualização do ambiente de redes, bem como, implementar protocolos de redes seguros, tais como SSH e HTTPS.

Art. 24. Planos de continuidade de negócios para recuperação de ataques de **malware**, incluindo **backups** e **softwares** necessários, devem ser mantidos pelos Elos do STI para seu escopo de atuação.

Art. 25. Procedimentos para coletar informações sobre novos **malwares**, devem ser implementados pelo Elo Especializado responsável pelo CTIR.FAB.

Art. 26. Os Elos do STI devem realizar, regularmente e de forma automatizada, **backup** de todos os dados de sistemas.

§ 1º As cópias de segurança devem ser armazenadas e protegidas em locais adequados, por meio de segurança física ou criptografados, conforme disposto nesta Política e no Termo de Ciência e Compromisso com as Políticas de Segurança da Informação, conforme consta no Anexo XIX.

§ 2º Devem ser executados testes de integridade dos dados e das mídias de armazenamento em período regular.

Art. 27. Os Elos do STI devem implementar, em seu escopo de atuação, medidas que detectam acessos a sites maliciosos ou suspeitos.

Art. 28. **Logs** e alertas do **software antimalware** devem ser armazenados pelos Elos do STI em um local seguro e o acesso deve ser restrito para evitar roubo ou vazamento de dados pessoais que tenham sido coletados.

Art. 29. O Órgão Central do STI deve especificar tipos de **softwares** preventivos (**antimalware**, antivírus, **firewall**) necessários para cada tipo de **host** (servidor, laptop, smartphone, pc etc.) e deve listar os requisitos para configuração e atualização deles.

Art. 30. Ameaças para tipos de **malware** que não exploram vulnerabilidades, como ataques de engenharia social, devem ser mitigados pelas Organizações do COMAER.

CAPÍTULO VII
CONFIGURAÇÃO E ATUALIZAÇÃO

Art. 31. É dever do Elo Especializado do STI responsável pelo CTIR.FAB manter um processo de configuração seguro para ativos corporativos, dispositivos de usuário final incluindo portáteis e móveis, dispositivos não computacionais/IoT, servidores e **softwares** como sistemas operacionais e aplicações.

Art. 32. O processo de configuração deve ser revisado e atualizado em períodos predefinidos ou quando ocorrer mudanças significativas no COMAER que possam impactar esta medida de segurança.

Art. 33. O Elo Especializado do STI responsável pelo CTIR.FAB deve realizar, de forma centralizada, o gerenciamento de **software antimalware** podendo conter agentes do **software antimalware** em ativos de informação como estação de trabalho e servidores.

Art. 34. É dever dos Elos do STI configurar e atualizar o **software** de detecção **antimalware** regularmente e realizar varredura nos computadores, servidores e mídias de armazenamento eletrônico incluindo:

I - dados recebidos por meio da rede ou qualquer mídia de armazenamento eletrônico; e

II - **e-mail**s, mensagens instantâneas e downloads.

Art. 35. Os Elos do STI devem configurar, o **software antimalware** para que ele obtenha as atualizações das bases **antimalware** de forma automática. Quando isso não puder ser realizado, deve ser devidamente justificado e aprovado pelo Órgão Central do STI.

Art. 36. É dever dos Elos do STI configurar, em seu escopo de atuação, os dispositivos para a não execução e reprodução automática de mídias removíveis.

Art. 37. Os Elos do STI devem configurar, os **softwares antimalware** para realizar a varredura automática de mídias removíveis quando inseridas nos dispositivos.

Art. 38. Devem ser configuradas, pelos Elos do STI, as funcionalidades "**anti-exploits**" que estejam disponíveis nos sistemas operacionais e a implementadas as ferramentas que possam ser configuradas para aplicar proteções sobre um conjunto mais amplo de aplicações e executáveis.

Art. 39. Os Elos do STI devem realizar o gerenciamento de controle de acesso em ativos que se conectam remotamente à organização, considerando, mas não se limitando a:

I - determinar a quantidade de acessos às soluções utilizando recursos de **softwares** e de rede;

II - possuir processos de configuração segura de ativos remotos; e

III - certificar-se que os sistemas operacionais, **software antimalware** e demais aplicações estejam sempre atualizados.

Art. 40. O STI pode utilizar **software antimalware** com função holística que tenha a capacidade de monitorar e identificar os comportamentos atípicos de seus ativos de informação.

Art. 41. É dever dos Elos do STI realizar a atualização de sistemas operacionais e **softwares** por meio de gestão automatizada de **patches**.

Art. 42. O Elo Especializado do STI responsável pelo serviço de **e-mail** corporativo deve configurar o **software antimalware** no servidor de **e-mail** para realizar a varredura de anexos e implementar um ambiente virtual controlado para realizar a verificação e abertura de anexos, tais como uma **sandbox**.

Art. 43. É dever dos Elos do STI remover ou alterar contas locais e senhas padrão de sistemas operacionais e **softwares** para evitar acessos não autorizados.

Art. 44. Os Elos do STI devem desativar ou remover serviços desnecessários, principalmente os serviços de rede, pois são vetores adicionais que um **malware** utiliza para se propagar.

Art. 45. Elo Especializado do STI responsável pelo serviço de **e-mail** corporativo deve configurar o servidor de **e-mail** para proibir o envio e recebimento de certos tipos de arquivos (Ex.: .exe.)

Parágrafo único. A lista de tipos de arquivos a serem bloqueados será proposta pelo Elo Especializado do STI responsável pelo CTIR.FAB e aprovada pelo Órgão Central do STI.

CAPÍTULO VIII
DETECÇÃO E ANÁLISE DE MALWARE

Art. 46. Os Elos do STI devem realizar verificação e validação regular de **softwares**, sistemas críticos e de dados de sistemas em busca de arquivos desconhecidos que não tenham sido aprovados ou alterações não autorizadas;

Art. 47. Deve ser divulgado amplamente, pelo Elo Especializado do STI responsável pelo CTIR.FAB, comunicados sobre ameaças e procedimentos que os usuários devem realizar ao detectar possíveis anormalidades nos ativos de informação.

Art. 48. É dever dos Elos do STI isolar o ambiente ou os ativos de informação suspeitos, infectados e os que podem ser potencialmente comprometidos para análise e identificação de **malware**.

Art. 49. O STI precisa investigar todo incidente onde haja suspeita de que a origem possa ser um **malware**, para verificar se essa é de fato a causa subjacente.

Art. 50. O Elo Especializado do STI responsável pelo CTIR.FAB deve identificar quais ativos de informação estão infectados por **malware**, para que assim, todos estes ativos consigam ser analisados e, consequentemente, ações específicas de contenção, erradicação e recuperação sejam realizadas.

Art. 51. É dever dos Elos do STI garantir que toda a identificação de infecção por **malware** seja realizada por meio de ferramentas automatizadas.

Art. 52. É dever dos Elos do STI classificar e nomear cuidadosamente os seus ativos de informação, de forma a tornar a detecção de **malware** mais eficaz.

Art. 53. O Órgão Central do STI deve determinar quais tipos de informações de identificação do ativo de informação são necessárias (IP, Sistema Operacional, localização física do ativo de informação), bem como quais fontes de dados dos sistemas de detecção serão utilizadas.

Art. 54. Os Elos do STI devem utilizar ferramentas de detecção do **malware** como SIEM, IDS, IPS, para identificar as características de ação do **malware**.

Art. 55. Os Elos do STI devem pesquisar informações sobre **malware** em fornecedores de antivírus, tais como:

I - categoria do **malware** (por exemplo, **worm**, **trojan**, vírus);

II - serviços, portas, protocolos que são explorados pelo **malware**;

III - como o **malware** impacta o ativo de informação infectado;

IV - vulnerabilidades que são exploradas pelo **malware**;

V - como o **malware** se propaga nos ativos de informação; e

VI - como realizar a contenção e remoção do **malware**.

Art. 56. Os Elos do STI podem utilizar **sniffers** de pacotes para realizar a busca ativa de um **malware** específico.

Art. 57. A equipe de segurança da informação dos Elos do STI deve analisar o comportamento do **malware** de forma ativa (ao executar o **malware** em um ambiente controlado) ou de forma forense (analisando as evidências de ações do **malware** no ativo de informação infectado).

§ 1º Caso a análise de **malware** seja por meio de ambiente controlado, o elo do STI deve estabelecer um sistema de testes isolado, sem acesso à sua rede corporativa e operacional.

§ 2º O sistema de testes deve ser estabelecido em um sistema operacional virtualizado do Elo do STI, que após a realização da análise de comportamento do **malware**, deverá ser apagado.

§ 3º O sistema de testes deve incluir ferramentas de identificação e detecção de **malware** atualizadas.

Art. 58. Os Elos do STI podem utilizar da análise de **logs** para analisar o comportamento de um **malware**.

Art. 59. Implementar ferramenta de análise de tráfego baseado em rede, como o sistema de prevenção de intrusão, buscando pacotes suspeitos, fluxos incomuns na rede e assinaturas de ataque, visando interromper a atividade potencialmente maliciosa.

Art. 60. Os Elos do STI devem utilizar tecnologias de inspeção e filtragem de conteúdo, tais como as especificadas a seguir:

VII - ferramenta de filtragem de spam;

VIII - ferramenta de filtragem e inspeção de conteúdo da web; e

IX - listas negras de sites maliciosos.

Art. 61. Os Elos do STI devem utilizar métodos de arquitetura defensiva, tais como:

I - proteção de **BIOS**; e

II - **SandBox**.

CAPÍTULO IX
REMEDIAÇÃO - CONTENÇÃO E ERRADICAÇÃO

Seção I
Da contenção

Art. 62. As estratégias de contenção devem apoiar os responsáveis pelo tratamento de incidentes na seleção da combinação apropriada de métodos, com base nas características de uma situação específica.

Art. 63. Os usuários devem receber instruções sobre como identificar infecções e quais medidas tomar se um **host** for infectado, tais instruções incluem e não se limitam a:

I - ligar para o Elo do STI responsável pelo suporte técnico;

II - desconectar o **host** da rede; e

III - desligar o **host.**

Art. 64. O **malware** identificado deve ser removido dos ativos do COMAER.

Art. 65. **Softwares** não autorizados devem ser removidos dos ativos do COMAER ou receber uma exceção documentada.

Art. 66. Todas as exceções devem ser anotadas no inventário de **software** e no registro de exceções.

Art. 67. Os Elos do STI devem ter mecanismos alternativos para distribuir informações aos usuários, como enviar mensagens para todas as caixas de correio de voz das OM apoiadas, afixar cartazes nas áreas de trabalho e distribuir instruções nas entradas dos edifícios e escritórios.

Art. 68. Os Elos do STI devem identificar e implementar métodos para fornecer utilitários e atualizações de **software** aos usuários que deverão ajudar na contenção.

Art. 69. É prudente que os Elos do STI utilizem tecnologias automatizadas para prevenir e detectar infecções, o que irá ajudar a conter muitos incidentes causados por **malwares**. Essas tecnologias incluem **softwares**, tais como antivírus, filtragem de conteúdo e prevenção de intrusões.

Art. 70. Os Elos do STI devem estar preparados para usar outras ferramentas de segurança para conter o **malware** até que as assinaturas antivírus possam realizar a contenção de forma eficaz.

Art. 71. Se o Elo Especializado do STI responsável por Segurança da Informação receber assinaturas atualizadas, é prudente testá-las pelo menos antes da implantação, para garantir que a atualização em si não cause um impacto negativo no COMAER.

Art. 72. Os Elos do STI podem adotar, também, vários métodos de detecção automatizados que não sejam **software** antivírus, tais como os seguintes:

I - filtragem de conteúdo;

II - **software ips** baseado em rede; e

III - lista negra executável.

Art. 73. Manter lista das portas TCP e UDP utilizadas por cada serviço, para que possa suportar a desativação de serviços de rede.

Art. 74. Manter uma lista de dependências entre os principais serviços para que a equipe de resposta a incidentes esteja ciente deles ao tomarem decisões de contenção.

Art. 75. Os Elos do STI podem parar serviços que estiverem com vulnerabilidades e oferecer outros alternativos com funcionalidades semelhantes aos usuários.

Art. 76. As ETIR devem considerar bloquear todo o acesso ao **host** externo (por endereço IP ou nome de domínio, conforme apropriado), se os **hosts** infectados tentarem estabelecer conexões com um **host** externo para baixar **malwares**, como por exemplo **rootkits**.

Art. 77. Se **hosts** infectados tentarem espalhar um **malware**, os Elos do STI poderão bloquear o tráfego de rede dos endereços IP dos **hosts** para controlar a situação enquanto os infectados são fisicamente localizados e limpos.

Art. 78. Os Elos do STI devem projetar e implementar as redes sob sua responsabilidade para tornar a contenção, através da perda de conectividade, mais fácil e menos perturbadora, isso poderá incluir:

I - colocar servidores e estações de trabalho em sub-redes separadas;

II - uso de redes locais virtuais (VLAN) separadas para **hosts** infectados.; e

III - segregação física de ativos críticos.

Art. 79. As ETIR devem selecionar uma combinação de métodos de contenção que, provavelmente, serão eficazes na contenção do atual incidente, ao mesmo tempo em que limita os danos aos **hosts** e reduz o impacto que os métodos de contenção podem ter sobre outros **hosts**.

Art. 80. As OM do COMAER devem apoiar decisões de contenção sólidas, tendo políticas que estabeleçam claramente quem tem autoridade para tomar decisões importantes de contenção e sob que circunstâncias (por exemplo, desconectar sub-redes da Internet).

Seção II
Da erradicação

Art. 81. Nos casos em que a destruição do **malware** é possível, as ferramentas mais comuns para erradicação empregadas pelo COMAER normalmente são: **software** antivírus, **software** de controle de acesso à rede e outras ferramentas projetadas para remover **malware** e corrigir vulnerabilidades.

Art. 82. Os Elos do STI podem utilizar métodos automatizados de erradicação, como acionar verificações de antivírus remotamente.

Art. 83. Os Elos do STI devem fornecer instruções e atualizações de **software** aos usuários além de assistência durante o processo de erradicação de **malwares**.

Art. 84. Os Elos de Serviço do STI podem manter áreas de suporte técnico formais ou informais nas principais instalações para aumentar a eficácia e eficiência na erradicação de **malwares**.

Art. 85. Durante incidentes graves, integrantes da equipe de TI podem ser realocados temporariamente de outras funções para ajudar nos esforços de erradicação.

Art. 86. Os Elos do STI devem estar preparados para reconstruir **hosts** rapidamente, conforme necessário, quando ocorrerem incidentes de **malware**.

Art. 87. Em vez de realizar ações típicas de erradicação, os Elos do STI devem reconstruir qualquer hospedeiro (ativo de TI) que apresente alguma das seguintes características de incidente:

I - um ou mais invasores obtiveram acesso de nível de administrador ao **host**;

II - o acesso não autorizado de nível de administrador ao **host** estava disponível para qualquer pessoa através de um **backdoor**, através de um compartilhamento desprotegido criado por um **worm** ou por outros meios;

III - os arquivos do sistema foram substituídos por um cavalo-de-tróia, **backdoor**, **rootkit**, ferramentas de ataque ou outros meios;

IV - o **host** fica instável ou não funciona corretamente depois que o **malware** foi erradicado por **software** antivírus ou outros programas ou técnicas. isso indica que o **malware** não foi completamente erradicado ou que causou danos a arquivos ou configurações importantes do sistema ou de aplicativos; e

V - há dúvidas sobre a natureza e a extensão da infecção ou sobre qualquer acesso não autorizado obtido por causa da infecção.

Art. 88. As ETIR devem realizar, periodicamente, atividades de identificação de hospedeiros que ainda estão infectados e estimar o sucesso da erradicação.

Art. 89. Os Elos do STI devem se esforçar para reduzir o número suspeito de máquinas infectadas e vulneráveis a níveis suficientemente baixos, para que, se todas elas estiverem conectadas a rede de uma só vez e todas as máquinas vulneráveis estiverem infectadas, o impacto geral das infecções seja o menor possível.

CAPÍTULO X
DA RECUPERAÇÃO

Art. 90. Os Elos do STI devem observar dois aspectos principais da recuperação de incidentes de **malware**, que são:

I - restaurar a funcionalidade e os dados dos **hosts** infectados; e

II - remover medidas de contenção temporárias.

Art. 91. Para incidentes de **malware** que são muito mais prejudiciais, como cavalos de Tróia, **rootkits** ou **backdoors**, que corrompem milhares de arquivos de sistema e de dados ou destroem discos rígidos, muitas vezes é melhor reconstruir primeiro o **host** e depois proteger o **host** para que ele não fique mais vulnerável à ameaça de **malware**.

Art. 92. Os Elos do STI devem considerar cuidadosamente os possíveis cenários de pior caso, como uma nova ameaça de **malware** que exija a reconstrução de uma grande porcentagem de suas estações de trabalho, e determinar como os **hosts** seriam recuperados nesses casos, isto pode incluir:

I - identificação de quem executaria as tarefas de recuperação;

II - estimativa de quantas horas de trabalho seriam necessárias e quanto tempo de calendário decorreria; e

III - determinação de como os esforços de recuperação deveriam ser priorizados.

Art. 93. Os Elos do STI devem determinar quando remover medidas de contenção temporárias.

Art. 94. As ETIR devem esforçar-se para manter medidas de contenção em vigor até que o número estimado de hospedeiros infectados e de hospedeiros vulneráveis à infecção seja suficientemente baixo, de modo que os possíveis incidentes subsequentes tenham poucas consequências.

Art. 95. As ETIR também devem considerar medidas de contenção alternativas que possam manter adequadamente a contenção do incidente e, ao mesmo tempo, causar menor impacto nas funções normais do COMAER.

Art. 96. As ETIR devem avaliar os riscos de restaurar os serviços.

Art. 97. O Órgão Central do STI deve, em última análise, ser responsável por determinar o que deve ser feito, com base nas recomendações da equipe de resposta a incidentes e na compreensão da gestão sobre o impacto no COMAER da manutenção das medidas de contenção.

CAPÍTULO XI
RELATÓRIOS E LIÇÕES APRENDIDAS

Art. 98. Todos os alertas de alta gravidade confirmados devem ser relatados ao Elo Especializado do STI responsável por Segurança da Informação.

Parágrafo único. O Elo Especializado deverá informar o Órgão Central do STI.

Art. 99. Os usuários devem ser treinados para reportar **malwares** descobertos ao seu respectivo Elo de Serviço do STI.

Art. 100. Possíveis resultados de atividades de lições aprendidas para incidentes de **malware** podem ser os seguintes:

I - mudanças na política de segurança;

II - mudanças no programa de conscientização;

III - reconfiguração de **software**;

IV - implantação de **software** de detecção de **malware**; e

V - reconfiguração do **software** de detecção de **malware**.

ANEXO XIX
TERMO DE CIÊNCIA E COMPROMISSO COM AS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO

COMANDO DA AERONÁUTICA
[Nome da OM].

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____ (nome completo), SARAM/CPF nº _____, lotado(a) na Organização Militar _____, declaro que li, compreendi e me comprometo a cumprir o disposto na NSCA 7-13 "Segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica" e das seguintes Políticas do COMAER nele anexas:

I - Política de Uso de Recursos Computacionais;

II - Política de Administração de Recursos Computacionais;

III - Política de Manipulação de Informações Classificadas;

IV - Política de Antivírus e Códigos Maliciosos;

V - Política de Firewall e Recursos Computacionais Localizados em Zonas Desmilitarizadas;

VI - Política de Segurança Física;

VII - Política de Segurança dos Serviços de Rede.

VIII - Política de Segurança em Servidores;

IX - Política de Acesso Remoto;

X - Política de Segurança Lógica;

XI - Política de Inspeção;

XII - Política de Backup e Restauração de Dados Digitais;

XIII - Política de Gestão de Ativos;

XIV - Política de Gestão de Dados;

XV - Política de Controle de Acesso;

XVI - Política de Gestão de Registros (logs) de Auditoria – PGRA;

XVII - Política de Defesa Contra Malware;

XVIII - Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação;

XIX - Política de Gerenciamento de Vulnerabilidades;

XX - Política de Gestão de Provedor de Serviços;

XXI - Política de Proteção de Dados Pessoais; e

XXII - Política de Acessibilidade Digital;

Declaro estar ciente de que qualquer violação das diretrizes e dos requisitos estabelecidos em tais políticas poderá resultar em ações legais ou disciplinares, nos termos da Lei 8.112/1990, Decreto-lei nº 1.002, de 21 de outubro de 1969 e Decreto nº 76.322, de 22 de setembro de 1975.

Por meio deste, manifesto minha concordância integral com as diretrizes estabelecidas e comprometo-me a atuar em conformidade com as políticas mencionadas.

Nome do Militar/Servidor

_____

Cargo/Função:

_____

Assinatura:

_____

Local e Data:

_____

AVISO DE PRIVACIDADE

O Comando da Aeronáutica coletará e tratará seus dados de acordo com a Lei 13.709 de agosto de 2018 (LGPD), com a **finalidade** de ceder acesso aos seus militares possuidores de larga experiência profissional e reconhecida competência técnico-administrativa, **limitando-se ao mínimo de dados** para a realização da contratação do referido serviço. Os dados **não serão compartilhados** por terceiros e nem utilizados fora da finalidade da coleta. **Os dados pessoais coletados ficarão constante em nossa base de dados e ao fim da vigência, as informações serão tratadas conforme o previsto nas leis arquivísticas vigentes.**

O requerente ao serviço, titular dos dados pessoais, concorda com o tratamento de seus dados pessoais para a finalidade determinada de forma livre e inequívoca.

ANEXO XX
POLÍTICA DE DESENVOLVIMENTO DE PESSOAS EM PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO

CAPÍTULO I
PROPÓSITO

Art. 1º A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação tem por objetivo estabelecer diretrizes, princípios e conceitos para conscientizar e capacitar os servidores e conscientizar colaboradores que se relacionam com o COMAER e que em algum momento têm acesso ou realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes, tais como o Decreto n° 9.991, de 28 de agosto de 2019 e o Decreto 9.637, de 26 de dezembro de 2018.

CAPÍTULO II
ESCOPO

Art. 2º A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação se aplica a todo o COMAER.

Art. 3º Esta Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação se aplica aos servidores e colaboradores do COMAER, incluindo gestores, prestadores de serviços, estagiários e contratados que tenham acesso e/ou utilize dados institucionais, incluindo os dados pessoais.

CAPÍTULO III
DECLARAÇÕES DA POLÍTICA

Seção I
Dos princípios gerais

Art. 4º A Política de Desenvolvimento de Pessoas em Privacidade e Segurança da Informação do COAMER deve permanecer alinhada:

I - com Lei Geral de Proteção de Dados Pessoais (Lei 13.709, de 14 de agosto de 2018);

II - com a Política Nacional de Desenvolvimento de Pessoas (Decreto 9.991, de 28 de agosto de 2019);

III - com a Política Nacional de Segurança da Informação (Decreto 9.637, de 26 de dezembro de 2018);

IV - com Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020;

V - com Instrução Normativa SGD/ME Nº 117, de 19 de novembro de 2020;

VI - com o Programa de Privacidade e Segurança da Informação (PPSI - Portaria SGD/MGI nº 852, DE 28 de março de 2023);

VII - com o Plano de Desenvolvimento de Pessoas do Órgão;

VIII - com a Política de Segurança da Informação do Órgão;

IX - com a Política de Proteção de Dados Pessoais do Órgão; e

X - com uma gestão de continuidade de negócios em nível organizacional.

Art. 5º Deve ser previsto pelo Órgão Central do STI, um número de atividades de conscientização, tais como, campanhas (por exemplo, “Dia da Privacidade e Segurança da Informação”) e a publicação de boletins ou folhetos.

Art. 6º Os treinamentos do COMAER, devem estar alinhados com as melhores práticas de tratamento de dados pessoais, privacidade e segurança da informação, em especial as recomendações do PPSI:

I - melhores práticas de tratamento de dados;

II - como reconhecer ataques de engenharia social;

III - melhores práticas de autenticação;

IV - causas da exposição não intencional de dados; e

V - como reconhecer e relatar incidentes de segurança.

Art. 7º As OM do COMAER devem definir, com assessoramento do Elo de Serviço do STI que as apoia, os níveis de conhecimento e habilidade necessários para os servidores e colaboradores executarem deveres e tarefas relacionadas a Privacidade e Segurança da Informação.

Art. 8º O planejamento das ações de desenvolvimento de pessoas em privacidade e segurança da informação do COMAER, deve estar de acordo com os princípios da economicidade e da eficiência, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019.

Seção II
Das metas e resultados esperados

Art. 9º As OM do COMAER, com assessoramento dos Elos de Serviço do STI que as apoia, devem:

I - promover o desenvolvimento pessoal em privacidade e segurança da informação;

II - estabelecer metas institucionais como referência para o planejamento das ações de desenvolvimento em privacidade e segurança da informação;

III - atingir um nível de conhecimento considerável em privacidade e segurança da informação, após sua conclusão; e

IV - avaliar o desempenho e comprometimento dos servidores com as metas e necessidades institucionais ao final de cada processo de desenvolvimento.

Seção III
Dos papéis e Responsabilidades

Art. 10. Cabe ao Órgão Central do STI a responsabilidade de planejar e coordenar a execução das atividades de ensino em privacidade e segurança da informação.

Art. 11. Cabe ao Gestor de Segurança da Informação do COMAER, estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação, conforme previsto no art. 19 da Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020.

Art. 12. Cabe ao Encarregado pelo tratamento de dados pessoais do COMAER, com apoio dos Encarregados de Coordenação dos ODGSA e dos Elos de Serviço do STI, orientar os funcionários e os contratados do COMAER, a respeito das práticas de desenvolvimento pessoal a serem tomadas em relação à proteção de dados pessoais.

Art. 13. Cabe à Alta Administração do COMAER, capacitar os Agentes Responsáveis (Controladores, Operadores e Encarregados dos Dados) para o uso dos recursos criptográficos, observando as normas vigentes, os procedimentos de credenciamento de segurança, e o tratamento de informação classificada.

Art. 14. Todos os servidores e colaboradores do COMAER, têm a responsabilidade de implementar os conceitos ensinados nos programas de conscientização e treinamento em Privacidade e Segurança da Informação.

Art. 15. Todas as ações de capacitação em Privacidade e Segurança da Informação, independentemente de sua fonte de recursos, devem ser acompanhadas pelo Órgão Central do STI.

Art. 16. O Órgão Central do STI deve divulgar periodicamente, por intermédio da Intraer ou por outros meios, os eventos constantes no Plano Anual de Capacitação do STI.

Art. 17. Cabe aos Comandantes, Chefes e Diretores de Organizações Militares com Elos do STI promover a indicação e matrícula dos militares de seu efetivo, conforme o Plano Anual de Capacitação do STI.

Seção IV
Do orçamento

Art. 18. Quanto às ações de desenvolvimento de servidores civis nas áreas de Privacidade e Segurança da Informação, o COMAER deve:

I - somente realizar despesas com ações de desenvolvimento de servidores civis do COMAER em privacidade e segurança da informação, após aprovação do PDP, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019;

II - racionalizar e utilizar de modo efetivo os recursos orçamentários destinados ao desenvolvimento de pessoas em privacidade e segurança da informação;

III - publicar na Internet, de forma transparente e objetiva, todas as despesas com as ações de desenvolvimento de servidores civis em privacidade e segurança da informação, conforme disposto no art. 16 do Decreto nº 9.991, de 28 de agosto de 2019; e

IV - analisar o custo-benefício das despesas realizadas no exercício anterior com as ações de desenvolvimento de pessoas em privacidade e segurança da informação, conforme disposto no art. 3º do Decreto nº 9.991, de 28 de agosto de 2019.

Art. 19. Quanto às ações de desenvolvimento dos militares nas áreas de Privacidade e Segurança da Informação, o COMAER deve:

I - as despesas com ações de desenvolvimento de militares nas áreas de privacidade e segurança da informação deverão ser norteadas pelo Plano Anual de Capacitação do STI.

Seção V
Das ações de desenvolvimento prioritárias

Art. 20. Durante a realização do planejamento das ações prioritárias de desenvolvimento de pessoas deve-se criar um quadro com a programação das atividades, no qual contenha para cada ação de desenvolvimento do servidor e/ou colaborador do COMAER:

I - nome do evento ou ação;

II - a carga horária;

III - tipo de atividade; e

IV - forma de realização.

Art. 21. As ações de desenvolvimento prioritárias do COMAER devem ser definidas dentre as relacionadas a seguir:

I - ações que visam ao atendimento às necessidades diagnosticadas com base em avaliações da instituição e, ou, de seu planejamento estratégico do COMAER;

II - curso introdutório financiado pelo COMAER, abordando os princípios básicos de Privacidade e Segurança da Informação na administração pública, entre outros;

III - treinamentos obrigatórios previstos em legislação específica sobre a temática de Privacidade e Segurança da Informação;

IV - ações destinadas ao desenvolvimento gerencial e reconhecimento de responsabilidades sobre proteção de dados;

V - ações que busquem elevar a maturidade e a resiliência do COMAER, em termos de privacidade e segurança da informação que permaneçam alinhadas com o PPSI;

VI - as ações de treinamento e conscientização realizadas pelo Órgão Central do STI, que visam a manter os servidores e/ou colaboradores atualizados sobre os desenvolvimentos no ambiente regulatório, contratual e tecnológico que possam afetar a conformidade de privacidade e de segurança da informação da organização;

VII - cursos de caráter permanente coordenados e realizados em parceria com as escolas de governo, outras instituições e/ou pessoas físicas direcionado a segurança da informação, privacidade e proteção de dados pessoais, conforme as funções das pessoas envolvidas com o tratamento de dados pessoais;

VIII - exercícios práticos de conscientização de segurança da informação que simulam ataques cibernéticos;

IX - conscientização de segurança da informação sobre reconhecimento e relato de potenciais indicadores de ameaça interna; e

X - treinamento em privacidade e segurança da informação baseado em funções para o servidor e/ou colaborador designando papéis e responsabilidades.

Seção VI
Dos procedimentos para solicitações de ações de desenvolvimento de pessoas

Art. 22. Os procedimentos para solicitações de ações de desenvolvimento de pessoas em privacidade e segurança da informação devem estar previstos em Plano de Desenvolvimento de Pessoas, no caso de servidores civis, ou no Plano Anual de Capacitação do STI, no caso de militares.

Art. 23. A solicitação para participação de militares ou servidores civis do COMAER, em ações de desenvolvimento deve ser feita via documento Oficial ao Órgão Central do STI, com posterior envio à DIRENS.

Art. 24. A participação em ação de desenvolvimento de pessoas por servidor civis do COMAER na área de privacidade ou segurança da informação que implicar em despesas diárias e passagens somente pode ser realizada se o custo total da ação for inferior ao custo da participação em evento similar na própria localidade de exercício do interessado, podendo ser aprovada, mediante justificativa, pelo comandante da OM daquele servidor civil.

Seção VII
Do afastamento para capacitação

Art. 25. É considerado afastamento para participação em ações de desenvolvimento do COMAER a:

I - licença para capacitação, nos termos do disposto no art. 87 da Lei nº 8.112, de 11 de dezembro de 1990;

II - participação em programa de pós-graduação stricto sensu no País, conforme o disposto no art. 96-A da Lei nº 8.112, de 11 de dezembro de 1990; e

III - realização de estudo no exterior, conforme o disposto no art. 95 da Lei nº 8.112, de 1990.

Art. 26. Os afastamentos podem ser concedidos pelas OM do COMAER, entre outros critérios, quando a ação de desenvolvimento:

I - estiver prevista no PDP da OM do servidor;

II - estiver alinhada ao desenvolvimento do servidor nas competências relativas ao Art. 19, II do Decreto Nº 9.991, de 28 de agosto de 2019; e

III - dispor de horário ou o local que inviabilize o cumprimento das atividades previstas ou a jornada semanal de trabalho do servidor.

Art. 27. Os afastamentos podem ser interrompidos, a qualquer tempo, a pedido do servidor ou no interesse da administração do COMAER.

Art. 28. A licença para capacitação do COMAER, deve observar a Lei Nº 8.112, de 11 de dezembro de 1990, o que consta no decreto Nº 9.991, de 28 de agosto de 2019 e demais normas correlatas.

ANEXO XXI
POLÍTICA DE GERENCIAMENTO DE VULNERABILIDADES

CAPÍTULO IV
ESCOPO

Art. 1º Esta Política de Gerenciamento de Vulnerabilidades se aplica aos sistemas e ativos informacionais do COMAER, incluindo funcionários, gestores, prestadores de serviços e contratados que tenham acesso e/ou utilizem ativos informacionais.

Seção I
Das exceções

Art. 2º Pode ocorrer que alguns ativos de informação do COMAER não serem contemplados por possíveis dificuldades técnicas ou obrigações contratuais e normativas. Quaisquer exceções a esta política deverão ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções do COMAER, a ser gerenciado pelo Órgão Central do STI.

Parágrafo único. Tais exceções devem ser tratadas no mapeamento de riscos de segurança da informação, em cumprimento ao Capítulo III da Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

Seção II
Do público

Art. 3º Esta Política se aplica a indivíduos responsáveis pela gestão e a indivíduos que utilizam qualquer Ativo de Informação da Rede Computadores em nome do COMAER. Além disso, a presente política se aplica a quaisquer provedores e entidades terceirizadas com acesso a informações, redes e aplicativos do COMAER.

CAPÍTULO V
DECLARAÇÕES DA POLÍTICA

Art. 4º Os sistemas e os dispositivos conectados à rede do COMAER, sejam eles próprios ou aqueles em processo de desenvolvimento e suporte por terceiros, devem passar periodicamente por varreduras em busca de vulnerabilidades que possam representar um risco para a infraestrutura e os dados sensíveis do COMAER.

Art. 5º Novas Soluções de TI construídos pelas equipes de desenvolvimento do COMAER ou de terceiros devem ser verificados no que concerne a vulnerabilidades antes de serem implantados no ambiente de produção.

Seção I
Do processo de gerenciamento de vulnerabilidades

Art. 6º Um processo de Gerenciamento de Vulnerabilidades deve ser criado, implementado, mantido e aplicado no COMAER.

Art. 7º O processo deve contemplar o gerenciamento de vulnerabilidades dos diversos ativos que sustentam os serviços da organização, incluindo a obtenção de informações oportunas sobre vulnerabilidades, a avaliação da exposição a tais vulnerabilidades e a implementação de salvaguardas apropriadas para lidar com o risco associado. Esses ativos abrangem, entre outros, a rede da organização, aplicações web, aplicativos móveis e sistemas operacionais.

Art. 8º O processo deve incluir atividades de suporte, incluindo, mas não se limitando a métricas de relatório e treinamento para implementação eficaz do PGV.

Art. 9º O processo deve incluir funções e responsabilidades das equipes/funções para realizar todas as atividades de maneira oportuna e eficaz para o COMAER.

Art. 10. O processo deve estabelecer mecanismos para obter atualizações de **software** quando emitidas pelo fabricante ou fornecedor oficial regularmente utilizando recursos autorizados, tais como sites de fornecedores de sistemas, fóruns e grupos de notícias, bancos de dados de gerenciamento de vulnerabilidades e diferentes ferramentas para rastrear as vulnerabilidades mais recentes.

Art. 11. A consistência e a eficácia do processo devem ser medidas por meio de métricas de gerenciamento de vulnerabilidades.

Art. 12. As métricas de gerenciamento de vulnerabilidades devem ser definidas pelo CGDSIPD e suas medições devem ser apresentadas a cada ano.

§ 1º Em síntese, as métricas são medidas baseadas em uma ou mais referências que servem para mensurar o grau de vulnerabilidade/ameaça em um determinado ativo de informação ou infraestrutura de TI.

§ 2º Algumas das métricas fundamentais (e não exaustivas) cujo acompanhamento é recomendado em uma estratégia de gerenciamento de vulnerabilidades abrangem:

I - cobertura;

II - tempo de detecção;

III - tempo de permanência;

IV - tempo para contenção ou atenuação;

V - número médio de vulnerabilidades ao longo do tempo;

VI - eficiência no gerenciamento de **patches**; e

VII - resultados de correção em relação ao Acordo de Nível de Serviço (ANS) da tabela de priorização de vulnerabilidades.

Seção II
Do mapeamento de ativos de informação

Art. 13. Um mapeamento de ativos de informação deve constar no escopo do processo de gerenciamento de vulnerabilidades e **patches** para determinar qual marca, modelo e versão de equipamento de **hardware**, sistemas operacionais, banco de dados, sistema, servidor **web** e aplicativos de **software** são usados no COMAER.

Art. 14. O mapeamento de ativos de informação deve ser atualizado anualmente ou sempre que ocorrerem alterações significativas para garantir que os recursos informacionais estejam cobertos pelo processo de gerenciamento de vulnerabilidades do COMAER.

Seção III
Da detecção de vulnerabilidades

Art. 15. As verificações de vulnerabilidade devem cobrir os ativos internos e externos à rede de produção.

Art. 16. As funções e as responsabilidades das equipes/funções para realizar atividades de detecção de vulnerabilidades devem ser estabelecidas.

Art. 17. As ferramentas devem ser configuradas e ajustadas adequadamente de acordo com o escopo avaliado.

Art. 18. Os tipos de varreduras e os tipos de teste devem ser avaliados e ajustados para que sejam congruentes com o escopo avaliado.

Art. 19. A frequência de testes de segurança deve levar em consideração os requisitos legais, regulamentares e contratuais que o COMAER deve cumprir e os riscos associados aos ativos avaliados.

Art. 20. As varreduras de vulnerabilidades na rede corporativa devem ser realizadas por períodos determinados ou após alteração significativa na rede, por equipe interna ou por terceiro ou uma combinação de ambos.

Art. 21. Os testes de segurança devem utilizar o feed de vulnerabilidade mais recente, de forma a evitar que determinadas vulnerabilidades não sejam detectadas.

Art. 22. Para cada teste, é necessário verificar a integridade da ferramenta utilizada e se ela varreu corretamente os ativos analisados e se existem exceções de vulnerabilidades.

Art. 23. As ferramentas utilizadas devem ser ajustadas continuamente, de forma a evitar que varreduras feitas por ferramentas distintas gerarem resultados distintos.

Art. 24. O teste de invasão ou o teste de penetração (**Pentest**) deve ser realizado conforme ato normativo específico do STI.

Art. 25. A integridade do resultado de detecção de vulnerabilidades deve ser avaliada antes de sua comunicação, de forma a evitar inconsistências, contradições ou resultados incompletos.

Art. 26. A detecção manual de vulnerabilidades deve ser considerada como complemento à detecção automática de vulnerabilidades.

Seção IV
Da elaboração e manutenção dos relatórios

Art. 27. As ETIR devem elaborar relatórios após cada ciclo de detecção para auxiliar o COAMER a entender e mensurar as vulnerabilidades existentes.

Art. 28. Os resultados da varredura devem passar por análise do CTIR.FAB com o dispositivo ou gerenciador de rede para que possíveis falsos positivos possam ser identificados e eliminados.

Art. 29. Grupos de ativos de informação devem ser determinados por tipo de ambiente, por tipo de sistema, por ID CVE ou por tipo de vulnerabilidade.

Art. 30. As ETIR devem adotar métricas para os relatórios de vulnerabilidade e determinar o valor percentual dos ativos de informação vulneráveis por gravidade e CVSS.

Art. 31. A quantidade e a porcentagem de novas vulnerabilidades devem ser monitoradas por: severidade; grupos funcionais; tipo de ambiente; tipo de sistema; autoridade de numeração CVE; e tipo de vulnerabilidade.

Art. 32. O relatório deve ser classificado, durante e após a sua elaboração, de acordo com a sensibilidade das informações presentes nele.

Art. 33. Todas as versões do relatório devem ser remetidas ao Órgão Central do STI para apreciação *do* gestor de segurança de informação do COMAER.

Seção V
Do banco de dados de vulnerabilidades

Art. 34. O Elo Especializado do STI responsável por Segurança da Informação deve manter um banco de dados de vulnerabilidades coletadas de várias fontes, como sites de segurança da informação, boletins de segurança ou publicações de fornecedores de **software**, que precisam ser aplicadas aos sistemas e ativos informacionais do COMAER.

Art. 35. O banco de dados poderá incluir informações de vulnerabilidade, análise de vulnerabilidade para priorização e plano de correção de vulnerabilidade.

Art. 36. O banco de dados deve ser atualizado regularmente com as informações mais recentes. As novas vulnerabilidades devem ser adicionadas ao banco de dados tão logo forem descobertas.

Art. 37. É recomendável que o banco de dados de vulnerabilidades seja integrado com outras ferramentas de segurança, como scanners de vulnerabilidades e sistemas de gerenciamento de **patches**. Isso ajuda a identificar e corrigir vulnerabilidades de forma mais rápida e eficiente.

Art. 38. As informações coletadas no banco de dados de vulnerabilidades devem ser analisadas regularmente para identificar tendências e padrões visando a tomada de medidas proativas para evitar futuras vulnerabilidades.

Seção VI
Da priorização e correção de vulnerabilidades

Art. 39. O tratamento de vulnerabilidades deve ser priorizado com base em sua classificação de risco e criticidade, tempo esperado para correção, grau de risco, impacto em caso de exploração e no valor que o ativo ou **host** impactado tem para o negócio das diversas áreas de atuação do COMAER.

Art. 40. As vulnerabilidades devem ser tratadas de acordo com o seu nível de severidade e nos prazos estipulados na Tabela de Classificação de Risco (Anexo XXII).

Art. 41. Os testes que forem concluídos com falha devem ser examinados novamente até que sua execução seja concluída com êxito. Caso não seja possível, deve-se avaliar se a vulnerabilidade será incluída na lista de exceções por pessoal autorizado, com base no processo de aceitação de risco.

Art. 42. A atualização de **softwares** deve ser realizada de forma tempestiva e eficiente, a fim de corrigir as vulnerabilidades conhecidas e reduzir a probabilidade de exploração por agentes maliciosos.

Art. 43. Quando as vulnerabilidades não puderem ser corrigidas dentro dos prazos estabelecidos nesta Política, o Elo Especializado responsável por Segurança da Informação deve enviar uma "solicitação de renúncia" ao Órgão Central do STI. A solicitação deve conter as seguintes informações:

I - detalhes do sistema ou ativo;

II - descrição detalhada da vulnerabilidade;

III - avaliação de risco que justifique a não correção imediata;

IV - a justificativa clara pela qual a correção não pode ser realizada no prazo estabelecido;

V - detalhes dos controles existentes (se houver);

VI - novo prazo de correção; e

VII - plano de ação da remediação (obedecendo o novo prazo de correção).

Art. 44. A decisão de aceitar ou rejeitar a solicitação de renúncia deve ser tomada pelo(a) Órgão Central do STI, com base na avaliação de risco apresentada. Se a solicitação de renúncia for aceita, a vulnerabilidade deve ser monitorada continuamente, pautado pelo plano de ação apresentado devendo ser corrigida assim que possível.

Art. 45. Os alertas de vulnerabilidades, as correções de **patches** e as ameaças emergentes que correspondam aos recursos informacionais relacionados no inventário de sistema e ativos de informação devem ser monitorados.

Seção VII
Das exceções

Art. 46. As exceções à Política de Gerenciamento de Vulnerabilidades, como para ativos de informação do COMAER não contemplados por esta política em função de dificuldades técnicas, obrigações contratuais e normativas ou outras razões legítimas, devem ser tratadas no mapeamento de riscos de segurança da informação, em cumprimento à Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021.

Art. 47. As exceções devem ser documentadas e aprovadas por meio de um processo de gerenciamento de exceções do COMAER.

Art. 48. A lista de exceções de ativos de informação deve ter validade de 1 (um) ano, devendo ser revisada após esse período.

Seção VIII
Dos registros de logs

Art. 49. Identificar quais eventos dos ativos de informação devem ser registrados, com base nos requisitos regulatórios, nas melhores práticas e nos objetivos do COMAER.

Art. 50. Ativos, físicos ou virtuais, como servidores e recursos de rede, devem recuperar informações baseadas em tempo de uma única fonte de tempo de referência (servidor NTP) regularmente para que os relógios de registro sejam consistentes.

Art. 51. As configurações referentes a ativos de informação devem incluir configurações de **log** para registrar ações que possam afetar ou que sejam relevantes para a segurança da informação.

Art. 52. Definir procedimento para análise de **logs**, como ferramentas de análise e correlação, para identificar possíveis ameaças e vulnerabilidades.

Art. 53. Uma revisão dos arquivos de registro (**logs**) deve ser conduzida pelo menos anualmente.

Art. 54. Os arquivos de registro (**logs**) devem ser protegidos contra adulteração e acesso não autorizado ou exfiltração.

Art. 55. Registros de **logs** dos sistemas e ativos informacionais classificados como críticos devem ser mantidos por pelo menos 1 ano.

Art. 56. Monitorar regularmente os registros de **logs** para identificar quaisquer tentativas de exploração de vulnerabilidades.

Art. 57. Registros de **log** devem ser excluídos de forma segura, garantindo que os registros sejam completamente apagados sem deixar vestígios ou dados remanescentes.

Seção IX
Da comunicação da ocorrência de vulnerabilidades e correções

Art. 58. As vulnerabilidades e respectivas informações de correção devem ser informadas aos usuários afetados, incluindo, mas não se limitando a: administradores de sistema, proprietários de sistema e usuários finais.

Art. 59. As correções bem-sucedidas de vulnerabilidades poderão ser testadas por meio de verificação de vulnerabilidades de rede e **host**, verificação de **logs** de **patches**, testes de invasão/penetração (**Pentest**) e verificação das definições de configuração.

Seção X
Da implementação e verificação das correções de vulnerabilidades

Art. 60. As correções de vulnerabilidades devem ser verificadas a saber se não há novas vulnerabilidades introduzidas. Isso pode ser feito por meio de testes de penetração, testes de vulnerabilidade e análise de **logs**.

Art. 61. Somente correções de vulnerabilidades que foram efetivamente testadas e aprovadas devem ser implantadas em produção. Atividades de correção de vulnerabilidades geralmente incluem, mas não se limitam à instalação de **patches** de segurança, bem como a ajustes de configuração e/ou remoção de **software**.

Art. 62. Quando instalações de **patches** de segurança e ajustes de configuração são recomendadas para mitigar as vulnerabilidades, elas devem ser enviadas por meio do processo de gestão de mudanças a ser definido em ato normativo do STI sobre Gestão de Ativos de Tecnologia da Informação no COMAER, para que os controles apropriados sejam implementados para teste, avaliação de riscos e reparação.

Parágrafo único. O Órgão Central do STI deverá publicar até 180 dias da publicação desta Política um ato normativo sobre Gestão de Ativos de Tecnologia da Informação no COMAER, alinhado com o PPSI.

Seção XI
Dos serviços em nuvem ou de terceiros

Art. 63. Para serviços em nuvem, as responsabilidades do provedor de serviços em nuvem pública com o cliente do serviço em nuvem devem ser definidas e acordadas.

Art. 64. Terceiros devem cumprir os requisitos desta Política de Gerenciamento de Vulnerabilidades. Sempre que possível, essa obrigação e outras responsabilidades que envolvam o gerenciamento de vulnerabilidades devem ser incluídas em contratos com terceiros.

ANEXO XXII
TABELA DE CLASSIFICAÇÃO DE RISCO

Nível de severidade	Prazo de correção	Descrição do risco
Muito Crítico (6)	2 dias	Condição totalmente inaceitável quando medidas imediatas devem ser tomadas para eliminar a materialização do risco e mitigar perigos e impactos.
Crítico (5)	30 dias	Pessoas mal-intencionadas podem facilmente obter o controle do **host**, o que pode comprometer toda a sua rede. As vulnerabilidades incluem acesso de leitura e gravação a arquivos, execução remota de comandos e **backdoors**.
Alto (4)	45 dias	Pessoas mal-intencionadas podem obter o controle do **host** ou coletar informações altamente confidenciais, incluindo acesso de "leitura" ao arquivo, **backdoors** em potencial ou uma lista de todas as contas de usuário no **host**.
Médio (3)	90 dias	Pessoas mal-intencionadas podem obter acesso às configurações de segurança no **host**, o que pode levar ao acesso a arquivos e à divulgação de conteúdo de arquivos, navegação em diretórios, ataques de negação de serviço e uso não autorizado de serviços.
Baixo (2)	120 dias	Pessoas mal-intencionadas podem coletar informações confidenciais do **host**, como versões de **software** instaladas, que podem revelar vulnerabilidades conhecidas.
Muito baixo (1)	180 dias	Pessoas mal-intencionadas podem coletar informações sobre o **host** por meio de portas ou serviços abertos, o que pode levar à divulgação de outras vulnerabilidades.

ANEXO XXIII
POLÍTICA DE GESTÃO DE PROVEDOR DE SERVIÇOS

CAPÍTULO I
PROPÓSITO

Art. 1º A Política de Gestão de Provedor de Serviços (PGPS) tem como objetivo fornecer diretrizes para auxiliar na avaliação, seleção, monitoramento e revisão dos provedores de serviços contratados, mitigando os riscos associados à terceirização e protegendo os ativos e informações do COMAER contra ameaças cibernéticas. A adoção da PGPS demonstra o compromisso do COMAER com a governança de serviços e com o estabelecimento de controles que minimizam riscos, fortalecendo a segurança cibernética e a resiliência operacional em um cenário digital cada vez mais complexo.

CAPÍTULO II
ESCOPO

Art. 2º Esta Política se aplica a todos os departamentos que contratam, supervisionam ou interagem com provedores de serviços externos. Isso inclui, mas não se limita a:

I - Tecnologia da Informação (TI) - responsáveis pela contratação e supervisão de provedores de serviços de infraestrutura de TI, hospedagem na nuvem, suporte técnico, entre outros.

II - Segurança Cibernética - encarregados de avaliar os riscos de segurança associados à terceirização de serviços e de implementar controles para mitigar esses riscos;

III - Defesa Cibernética - encarregados de avaliar os riscos associados à terceirização de serviços associados às atividades de Defesa Cibernética no COMAER;

IV - departamentos jurídicos e de compliance - responsáveis por revisar e avaliar contratos com provedores de serviços para garantir conformidade com regulamentações relevantes e requisitos legais;

V - compras e aquisições - encarregados do processo de licitações e contratação de provedores de serviços, em conformidade com as políticas e procedimentos estabelecidos; e

VI - todas as partes interessadas que interagem com os serviços fornecidos pelos provedores externos, incluindo funcionários, clientes e parceiros comerciais.

Art. 3º É fundamental que todas as áreas do COMAER que tenham envolvimento direto ou indireto com provedores de serviços externos sigam as diretrizes estabelecidas nesta Política. Isso garante uma abordagem consistente e coordenada para mitigar os riscos associados à terceirização de serviços e proteger os interesses e ativos do COMAER.

CAPÍTULO III
DECLARAÇÕES DA POLÍTICA

Art. 4º Esta política, alinhada com o Controle 15 do Guia de Framework de Privacidade e Segurança da Informação, adota uma abordagem proativa para mitigar os riscos associados à terceirização de serviços e garantir a segurança cibernética e operacional do COMAER.

Art. 5º As diretrizes a seguir podem ampliar os requisitos e práticas recomendadas para garantir a privacidade e segurança da informação ao gerenciar provedores de serviços, abrangendo áreas

como seleção, contratação, monitoramento, gerenciamento de incidentes, treinamento e conscientização.

Art. 6º Esta Política adota uma abordagem proativa para mitigar os riscos associados à terceirização de serviços e garantir a segurança cibernética e operacional do COMAER. Ao seguir esses princípios gerais, o COMAER irá fortalecer sua postura de segurança e proteger seus ativos críticos contra ameaças cibernéticas.

Seção I
Das diretrizes gerais

Art. 7º Esta PGPS demonstra aspectos micro e macro de privacidade, proteção de dados e segurança da informação na relação do COMAER com seus provedores de serviços de tecnologia da informação.

Art. 8º O Comitê de Governança Digital, de Segurança da Informação e de Proteção de Dados (CDGSIPD) estipulou o prazo de 2 (dois) anos para que as Organizações do COMAER e provedores de serviço se adequem às diretrizes desta PGPS.

Art. 9º Esta PGPS e suas atualizações deverão ser aprovadas pelo CGDSIPD.

Art. 10. Esta PGPS deve ser devidamente divulgada e estará disponível para todos os colaboradores do COMAER na página do STI na Intraer.

Art. 11. Os compromissos de melhoria contínua dos provedores de serviço devem permanecer expostos na PGPS.

Art. 12. Esta PGPS deverá ser revisada e atualizada de forma periódica, ou quando houver necessidade por motivos que o COMAER julgar relevantes (como por exemplo, adequação a novas leis, boas práticas, incidentes de segurança).

Art. 13. A organização deverá seguir as orientações da Instrução Normativa SGD/ME nº 94 para a gestão e governança de contratos de prestação de serviços.

Art. 14. A avalição de provedores de serviço deverá ser realizada levando em consideração, mas não se limitando, as diretrizes da Instrução Normativa SGD/ME nº 94.

Art. 15. A organização deverá estabelecer nos requisitos de contratação de provedores de serviços os aspectos mínimos e relevantes de proteção de dados e segurança da informação.

Art. 16. Os acordos e contratos entre o COMAER e os provedores devem ser estabelecidos e documentados para que haja um entendimento claro entre as partes sobre as obrigações de cumprimento os requisitos mínimos e relevantes de proteção de dados e segurança da informação.

Art. 17. Os acordos e contratos devem conter os seguintes termos de segurança da informação e proteção de dados:

I - descrição das informações a serem fornecidas ou acessadas e os métodos e meios de fornecimento ou acesso as estas informações aos provedores;

II - classificação das informações de acordo com o esquema de classificação das informações do COMAER;

III - mapeamento e análise de convergência entre o método de classificação de informações do COMAER e do provedor de serviços;

IV - requisitos mínimos de segurança da informação em relação a infraestrutura de ti do provedor;

V - requisitos e procedimentos para a gestão de incidentes de segurança da informação e violação de proteção de dados e privacidade; e

VI - contatos relevantes de ambas as partes, para possível tratamento de incidentes.

Art. 18. O COMAER deve definir um plano de ação para mitigar não conformidades de um provedor quando forem identificadas por meio de monitoramento.

Art. 19. O COMAER deve definir em seus contratos com provedores de serviços as obrigações de cada parte contratual de implementar um conjunto de controles acordados, incluindo controle de acesso, análise crítica de desempenho, monitoramento, relatos e auditorias, e as obrigações do provedor de serviços de estar em conformidade com os requisitos de proteção de dados e segurança da informação do COMAER.

Art. 20. O COMAER deverá implementar um processo de monitoramento com métodos estabelecidos para a validação de serviços e produtos em conformidade com os requisitos de proteção de dados e segurança da informação pré-estabelecidos.

Seção II
Da avaliação de riscos

Art. 21. A avaliação de riscos poderá ocorrer antes e durante o contrato com um provedor de serviços.

Art. 22. As OM do COMAER devem conduzir uma avaliação detalhada dos riscos associados à terceirização de serviços. Isso inclui, mas não se limita, a uma análise de vulnerabilidades potenciais, conformidade regulatória e impacto nas operações do COMAER.

Art. 23. O Encarregado da proteção de dados do COMAER deve estabelecer processos e procedimentos para gerenciar a proteção de dados e a segurança da informação e os riscos que podem ser associados com o uso de serviços e produtos de provedores.

§ 1º Devem ser estipulados os responsáveis pela avaliação.

§ 2º Deve ser definido quando os resultados da avaliação serão analisados e por quem.

§ 3º Deve ser definido como ocorrerá a análise dos relatórios elaborados após as avaliações e auditorias de seus provedores de serviço.

Art. 24. Deve ser definido como serão avaliados e gerenciados os riscos à proteção de dados e à segurança da informação associados a:

I - uso das informações internas por provedores e seus associados; e

II - vulnerabilidades e mal funcionamento de produtos ou serviços operados e criados pelos provedores e seus associados. (por exemplo, **software**, API, componentes de **hardware** e utilizados para a manutenção ativa dos produtos e serviços).

Art. 25. Devem ser implementadas ferramentas de análise de risco contínuo para identificar e mitigar proativamente novas ameaças à segurança de dados apresentadas pelos provedores de serviços.

Art. 26. Deverá ser realizada a gestão de risco adequada em cada fornecedor e seus respectivos serviços.

Art. 27. A avaliação pode ser realizada novamente após a ocorrência de um incidente de segurança.

Seção III
Dos contratos e acordos

Art. 28. Os acordos e contratos entre o COMAER e os provedores de serviço devem ser estabelecidos e documentados para que haja um entendimento claro entre a organização e o provedor de serviços sobre as obrigações de cumprimento dos requisitos mínimos e relevantes de proteção de dados e segurança da informação.

Art. 29. Os contratos dos provedores de serviços devem incluir, pelo menos, os seguintes requisitos de segurança:

I - requisitos mínimos do programa de segurança;

II - notificação e resposta a incidentes de segurança e/ou violação de dados;

III - criptografia de dados; e

IV - compromissos de descarte de dados.

Parágrafo único. Esses requisitos de segurança devem ser consistentes com esta Política.

Art. 30. A segurança deve ser implementada nas fases iniciais do desenvolvimento da PGPS, visando a economicidade, pois pode se tornar cara a longo prazo se for negligenciada.

Art. 31. Deve-se certificar de que os provedores de serviços considerados incorporem padrões de segurança do setor, como a ISO 27001.

Art. 32. Recomenda-se revisar contratos dos provedores de serviços anualmente para garantir que os contratos não faltem aos requisitos de segurança.

Art. 33. Todos os contratos com provedores de serviços devem incluir cláusulas específicas relacionadas à privacidade, proteção de dados, segurança da informação, responsabilidades, conformidade regulatória e requisitos de relatórios.

Art. 34. Quando necessário, os responsáveis pelas áreas de negócio do COMAER estabelecerão procedimentos para a continuação da prestação de serviço, em sua respectiva área, em caso de alteração do provedor, seja por conclusão do contrato ou por incapacidade do provedor original.

Art. 35. As OM do COMAER devem solicitar a assinatura de termos de confidencialidade por parte dos funcionários e colaboradores dos provedores de serviço, sendo esta, uma condição a ser cumprida antes dos associados do provedor de serviço iniciarem a operação de serviços e produtos.

Art. 36. Os contratos devem ser revisados por profissionais jurídicos e de segurança cibernética para garantir que as obrigações sejam claramente definidas e aplicáveis.

Art. 37. Dever constar nos instrumentos contratuais, cláusulas que estabeleçam o direito do COMAER de auditar as práticas de proteção de dados e segurança da informação do provedor de serviços.

Art. 38. Deve ser estabelecido um mecanismo para revisar e atualizar periodicamente os requisitos de privacidade, proteção de dados e segurança da informação do contrato à medida que novas ameaças e regulamentações surjam.

Art. 39. Devem ser definidos em contrato os recursos de TI e informações que os provedores de serviços podem acessar, usar, monitorar ou controlar.

Art. 40. Devem ser definidos e cumpridos os prazos de confidencialidade das informações, produtos e serviços do COMAER.

Art. 41. Deve ser definido em contrato o nível de segurança física e lógica esperado dos provedores e associados e suas instalações.

Art. 42. O Órgão Central do STI deve definir os requisitos de segurança da informação que serão utilizados para adquirir produtos ou serviços de TI em ato normativo específico sobre Contratações de Tecnologia da Informação no COMAER;

Art. 43. Deve ser exigido, contratualmente, que seus provedores propaguem e façam cumprir os requisitos de proteção de dados e segurança da informação do COMAER em toda a cadeia de fornecimento;

Art. 44. Solicitar que os provedores de produtos e serviços de TI forneçam informações descrevendo os controles de proteção de dados e segurança da informação implementados em seus produtos e serviços e as configurações necessárias para a sua operação segura;

Art. 45. Devem ser estabelecidos processos de fiscalização específicos para as contratações de TI com o objetivo de garantir que os produtos e serviços de TI entregues estejam funcionando como o esperado antes do pagamento pelo serviço.

Art. 46. Devem ser especificadas em contrato as responsabilidades do provedor de serviços em relação à exclusão segura de dados ao final do contrato ou quando não forem mais necessários.

Art. 47. Devem ser incluídas disposições contratuais que garantam a conformidade do provedor de serviços com as diretrizes de segurança de dados disposto na seção II (Da responsabilidade) da Lei Geral de Proteção de Dados - LGPD.

Art. 48. Devem ser estabelecidos protocolos para revisão e aprovação de quaisquer subcontratados ou provedores de serviços adicionais que o provedor de serviços possa envolver.

Art. 49. Devem ser definidos procedimentos para resolver divergências relacionadas à proteção de dados e à segurança da informação entre o COMAER e os provedores de serviços.

Seção IV
Dos provedores de serviço

Art. 50. Após a identificação e documentação dos potenciais provedores de serviços que atendam a esta Política, os Elos do STI devem proceder a classificação deles para fins de inventário de Provedores de Serviços em seu escopo de atuação, encaminhando as informações ao Órgão Central do STI.

Subseção I
Do inventário de provedores de serviço

Art. 51. O STI deve criar e manter um inventário de provedores de serviço e seus ativos associados, incluindo o número do contrato, tipo de serviço contratado, quantidade de operadores, e habilidades dos operadores.

Art. 52. O Órgão Central do STI deve promover a atualização do inventário a cada ano e quando ocorrerem novas contratações, alterações e encerramento de contratos.

Art. 53. O inventário é um ativo de informação como um catálogo de serviços, e devem ser aplicados controles de privacidade, proteção de dados e segurança da informação para evitar acessos indevidos, adulterações de conteúdo e vazamento de informações.

Art. 54. O inventário deve conter informações sobre os ativos de informação necessários a serem utilizados pelos provedores para a entrega e operação de serviços.

Parágrafo único. Compete aos Elos do STI, com apoio das OM contratantes das Soluções de TI, a realização do levantamento dessas informações e o encaminhamento delas ao Órgão Central do STI.

Art. 55. O Órgão Central do STI deve manter um inventário completo dos provedores de Serviço de TI do COMAER para fins de controle e eventual aplicação em processos de Mobilização.

Subseção II
Classificação de provedores de serviço

Art. 56. A classificação dos provedores de serviço deve ser realizada a cada ano.

Art. 57. O Órgão Central do STI estabelecerá como serão classificados os provedores de serviço de acordo com a sensibilidade das informações, produtos e serviços utilizados pelos provedores.

Art. 58. O Órgão Central do STI estabelecerá definir os tipos de componentes de serviços de infraestrutura de TI e nuvem fornecidos pelos fornecedores que podem degradar a proteção de dados e segurança da informação.

Art. 59. Os provedores de serviço devem ser classificados de acordo com a criticidade do serviço prestado para o COMAER.

Parágrafo único. Os responsáveis pela gestão do contrato devem auxiliar o processo de classificação dos provedores de serviço.

Art. 60. Deve ser registrado o grau de sensibilidade dos dados processados pelo provedor de serviços bem como os riscos associados à prestação de serviço.

Art. 61. A classificação deverá ser atualizada a cada ano ou quando ocorrerem mudanças significativas nas execuções dos contratos que possam impactar esta salvaguarda.

Art. 62. O Órgão Central do STI deve avaliar a necessidade de criar grupos de provedores de acordo com suas classificações, para que assim, sejam aplicadas medidas de privacidade, proteção de dados e segurança da informação específicas para cada grupo.

Art. 63. Os procedimentos para Classificação do Provedores de Serviço de TI serão detalhados em ato normativo específico do STI.

Seção V
Da avaliação e do monitoramento contínuo

Art. 64. O provedor de serviços deve permitir que a organização monitore e avalie a adesão e cumprimento aos requisitos contratuais por parte do provedor, principalmente de proteção de dados e segurança da informação.

Art. 65. Os provedores de serviços devem ser reavaliados de forma contínua.

Art. 66. As Equipes de Fiscalização de contratos, com apoio dos Elos do STI, devem avaliar se os requisitos de proteção de dados e segurança da informação estão sendo cumpridos com cada provedor e contrato de forma individual.

Art. 67. Os Elos do STI devem avaliar a qualidade e eficiência dos provedores de serviço de acordo com produtos e serviços entregues e em execução.

Art. 68. Devem ser realizadas avaliações, utilizando-se ou não de terceiros independentes, para verificar a conformidade do provedor de serviços com as normas de proteção de dados e segurança da informação.

Art. 69. Deve ser implementado no COMAER um processo de monitoramento contínuo para avaliar o desempenho dos provedores de serviços em relação aos padrões acordados de privacidade, proteção de dados, segurança da informação e conformidade regulatória.

Art. 70. O monitoramento pode envolver auditorias regulares, revisões de relatórios de segurança e testes de penetração.

Art. 71. O Órgão Central do STI, conjuntamente com o Encarregado da proteção de dados pessoais do COMAER, determinará o que deve ser monitorado e medido, incluindo processos, controles e requisitos de proteção de dados e segurança da informação.

Art. 72. O COMAER deve buscar desenvolver métodos para o monitoramento que consigam gerar resultados válidos e comparáveis devem ser definidos pela organização.

Art. 73. Os Elos do STI deverão realizar o monitoramento contínuo dos provedores de serviços e suas soluções de TI em seu escopo de atuação.

Art. 74. Os resultados do monitoramento e de medições devem ser analisados pelo Órgão Central do STI anualmente.

Art. 75. Todo monitoramento deve ser documentado e retido como evidência dos resultados, tendo uma cópia enviada ao Órgão Central do STI.

Art. 76. O monitoramento de conformidade do provedor de serviços pode ser implementado de maneira automatizada por meio de soluções de gerenciamento de riscos e conformidade.

Art. 77. Os registros detalhados de todas as interações com o provedor de serviços, incluindo comunicações, incidentes de segurança e auditorias deve ser mantidos por pelo menos 5 (cinco) anos, a partir da data de registro, exceto se constatadas obrigações adicionais que demandem maior prazo de manutenção.

Art. 78. Deverá ser utilizada a Solução de TI padronizada pelo COMAER para o gerenciamento dos contratos de TI de forma a possibilitar que as autoridades responsáveis recebam alerta precoce sobre quaisquer anomalias ou comportamentos suspeitos por parte do provedor de serviços que sejam percebidos pelas Equipes de Fiscalização.

Art. 79. O inventário organizado dos provedores de serviços deve ser mantido atualizado de forma a permitir identificar um ponto de contato com cada prestador de serviços.

Art. 80. Os provedores de serviços devem ser listados, classificados e designados em contato formal para cada provedor de serviços.

Art. 81. A revisão e atualização do inventário de provedores de serviços deve ser feita a cada ano ou quando ocorrerem mudanças significativas que possam impactar esta salvaguarda.

Art. 82. Desenvolver painéis de controle personalizados para visualizar métricas de privacidade, proteção de dados e segurança da informação em tempo real relacionadas aos provedores de serviços.

Art. 83. Devem ser realizados processos abrangentes de diligência (**due diligence**) para avaliar a credibilidade, reputação e práticas de segurança cibernética do provedor de serviços. Isso envolve revisar suas políticas de segurança, histórico de incidentes de segurança e certificações relevantes.

Art. 84. As OM do COMAER poderão utilizar a avaliação dos serviços e produtos prestados pelos provedores de serviço para verificar se estes atingiram os níveis de proteção de dados e segurança da informação necessários.

Seção VI
Da gestão de incidentes

Art. 85. Devem ser tratados em ato normativo específico do STI sobre Gestão de Incidentes Cibernéticos os seguintes tópicos:

I - requisitos mínimos de notificação de incidentes de segurança de dados pelo provedor de serviços, incluindo prazos e formato da comunicação.

II - procedimentos claros e responsabilidades para lidar com incidentes de segurança cibernética relacionados aos serviços fornecidos pelo provedor, incluindo:

a) a comunicação eficaz;

b) investigação de incidentes; e

c) ações corretivas para mitigar danos e evitar recorrências.

III - tratamento de incidentes de segurança da informação e violações a proteção de dados e privacidade que por algum motivo estejam correlacionados a algum provedor de serviços; e

IV - medidas de recuperação, contingência e resiliência cibernética para garantir a disponibilidade do tratamento de dados e informações dos provedores e do COMAER.

Art. 86. Devem ser mitigadas quaisquer ações dos provedores de serviços que venham a causar dano ao COMAER, independente da maneira que este tenha tomado conhecimento da ação.

Art. 87. Deve ser realizada a integração dos planos de resposta aos incidentes em comum com os provedores de serviços para facilitar a coordenação e colaboração durante incidentes de segurança de dados.

Art. 88. Devem ser designados pontos de contato dedicados entre o COMAER e o provedor de serviços para facilitar a comunicação e a troca de informações durante incidentes de segurança.

Art. 89. Devem ser implementadas simulações regulares de incidentes de segurança com o provedor de serviços para garantir uma resposta coordenada e eficaz.

Art. 90. Devem ser documentadas todas as interações e atividades relacionadas à resposta a incidentes com o provedor de serviços para fins de revisão e análise pós-incidente.

Art. 91. Deve ser estabelecido pelo Órgão Central do STI um protocolo claro para a condução de investigações conjuntas com o provedor de serviços para identificar a causa raiz de incidentes de segurança.

Art. 92. Revisões pós-incidente devem ser realizadas em colaboração com o provedor de serviços para identificar áreas de melhoria nos processos de resposta a incidentes.

Art. 93. Treinamento regular deve ser fornecido aos colaboradores sobre os procedimentos de notificação de incidentes e como interagir com o provedor de serviços durante um incidente de segurança.

Seção VII
Da revisão e melhoria contínua

Art. 94. Esta PGPS dever ser revisada a cada ano para garantir sua eficácia contínua e alinhamento com as melhores práticas de privacidade, proteção de dados e segurança da informação.

Art. 95. O Órgão Central do STI deve manter-se atualizado sobre a legislação e melhores práticas de mercado em relação a gestão de provedores de serviço e adaptar as políticas conforme necessário para manter a relevância e eficácia.

Art. 96. Os Elos do STI deverão criar um Objeto no Sistema de Atendimento ao Usuário (SAU), de nome “Qualidade dos Serviços de TI dos Provedores.” Para servir como canais de comunicação para receber **feedback** contínuo dos usuários internos e externos sobre a qualidade dos serviços dos provedores.

§ 1º Os integrantes das equipes de fiscalização dos contratos desse Serviços de TI devem ser incluídos como solucionadores desse objeto.

§ 2º Os chamados abertos para esse objeto serão analisados por integrante do Elo do STI responsável e encaminhados para os respectivos fiscais de contrato via SAU.

Art. 97. Lições aprendidas com incidentes passados e mudanças no ambiente operacional devem ser incorporadas para aprimorar os processos e controles.

Art. 98. O processo formal para revisão e validação dos relatórios de conformidade fornecidos pelo provedor de serviços deverão constar em ato normativo específico sobre Contratações de Tecnologia da Informação no COMAER.

Seção VIII
Do treinamento e conscientização

Art. 99. Para garantir que todos os colaboradores estejam devidamente informados e capacitados sobre a gestão de provedores de serviços, o Órgão Central e os Elos do STI devem implementar as seguintes medidas:

I - desenvolver materiais de treinamento personalizados para colaboradores de diferentes níveis e funções, em seu escopo de atuação, sobre a gestão de provedores de serviços;

II - realizar, em seu escopo de atuação, sessões de treinamento interativo e workshops para simular cenários práticos envolvendo provedores de serviços e práticas recomendadas de segurança;

III - avaliar, conjuntamente com as OM apoiadas, a possibilidade de estabelecer um programa de recompensas e reconhecimento para funcionários que demonstrarem um bom entendimento e adesão às políticas de gestão de provedores de serviços;

IV - fornecer recursos online acessíveis, como vídeos, guias e FAQs, para facilitar o aprendizado contínuo sobre segurança de dados e gestão de provedores de serviços;

V - coordenar, em seu escopo de atuação, a incorporação de treinamento sobre gestão de provedores de serviços e segurança de dados em programas de integração de novos funcionários e treinamentos regulares de reciclagem;

VI - avaliar, conjuntamente com as OM apoiadas, a possibilidade de realizar avaliações periódicas de conhecimento e conscientização entre os funcionários para medir a eficácia do treinamento sobre gestão de provedores de serviços;

VII - incentivar a participação em eventos e conferências do setor relacionados a proteção de dados e segurança da informação para promover a educação contínua e a conscientização;

VIII - acompanhar, junto às equipes de fiscalização, o encerramento de Contratos de TI;

IX - o provedor de serviço deverá realizar atividades para o descarte seguro de dados e informações nos ativos de informação que estão sob sua responsabilidade ou foram utilizados para a prestação de serviço;

X - contratos que utilizem a locação de ativos computacionais devem estabelecer o estado de preservação quando o ativo for devolvido;

XI - definir requisitos para garantir o término seguro de relacionamentos com os provedores e associados, incluindo, mas não se limitando a:

a) tratamento de informações;

b) desprovisionamento de direitos de acessos;

c) determinação da propriedade intelectual dos artefatos desenvolvidos durante o contrato;

d) possível portabilidade e repasse de informações em caso de alteração de provedor ou internalização de serviços;

e) atualização do inventário de provedores;

f) gerenciamento de registros;

g) devolução de ativos de informação; e

h) descarte e eliminação segura de informações e ativos de informação utilizados pelos provedores e seus associados.

XII - o prestador de serviço deverá realizar a limpeza segura dos ativos de informação utilizados no contrato.

ANEXO XXIV
POLÍTICA DE PROTEÇÃO DE DADOS PESSOAIS

CAPÍTULO I
PROPÓSITO

Art. 1º Esta Política de Proteção de Dados Pessoais tem por objetivo estabelecer diretrizes, princípios e conceitos a serem seguidos por todas as pessoas e entidades que se relacionam com o COMAER que em algum momento realizam operações de tratamento de dados pessoais, visando o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e outras normas vigentes.

CAPÍTULO II
ESCOPO

Art. 2º Esta Política se aplica a todas às OM do COMAER e tem a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Art. 3º Esta Política regula a proteção de dados pessoais, que o COMAER é o agente de tratamento, bem como o meio utilizado para este tratamento, seja digital ou físico, além de qualquer pessoa que realize operações de tratamento de dados pessoais em seu nome ou em suas dependências.

CAPÍTULO III
DECLARAÇÕES DA POLÍTICA

Art. 4º A presente Política tem como base legal a finalidade de estabelecer princípios e diretrizes para a implementação de ações que garantam a proteção de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Art. 5º Esta Política aplica-se a todas às OM do COMAER, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Ciência e Compromisso com as Políticas de Segurança da Informação (Anexo XIX), para acessar os ativos de informação sob responsabilidade do COMAER.

Art. 6º A aplicação desta Política será pautada pelo dever de boa-fé e pela observância dos princípios previstos no art. 6º da Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

CAPÍTULO IV
DAS DISPOSIÇÕES GERAIS

Art. 7º São objetivos desta Política de Proteção de Dados Pessoais:

I - estabelecer medidas eficazes para o cumprimento das normas de proteção de dados pessoais e demonstrar a eficácia das mesmas;

II - estabelecer revisões de processos com o objetivo de aferir a diminuição ou aumento de riscos que envolvem o tratamento de dados pessoais;

III - promover a administração dos dados pessoais coletados e tratados, em qualquer meio, físico ou digital, custodiados ou sob orientação direta ou indireta do COMAER, de acordo com as diretrizes especificadas;

IV - estabelecer a necessidade de criar e manter um registro de todas as operações de tratamento de dados pessoais realizados;

V - promover a adequada gestão do tratamento dos dados pessoais;

VI - promover a criação de programas de treinamento e conscientização para que os colaboradores entendam suas responsabilidades e procedimentos na proteção de dados pessoais; e

VII - promover a formulação regras de segurança, de boas práticas e de governança com objetivo de definir procedimentos e outras ações referentes a privacidade e proteção de dados pessoais.

Art. 8º As OM do COMAER registrarão e gravarão as preferencias e navegações realizadas nas respectivas páginas para fins estatísticos e de melhoria dos serviços ofertados, através de arquivos (cookies), respeitando o consentimento do titular.

Art. 9º São responsabilidades da Estrutura de Governança de Proteção de Dados Pessoais do COMAER:

I - atender ao disposto nos normativos e publicações da Autoridade Nacional de Proteção de Dados Pessoais (ANPD) que disciplinam o tratamento e a governança dos dados pessoais;

II - elaborar, quando couber, o Relatório de Impacto de Proteção de Dados Pessoais (RIPD) relacionados às operações de tratamento, e atualizá-lo quando necessário; e

III - realizar o desenvolvimento e a atualização das políticas/avisos de privacidade, que tem por finalidade o fornecimento de informações sobre o tratamento de dados pessoais em cada ambiente físico ou virtual, bem como, especificar as medidas de proteção de dados adotadas para salvaguardar esses dados pessoais.

CAPÍTULO V
TRATAMENTO DE DADOS PESSOAIS

Art. 10. O tratamento de dados pessoais deve ser sempre realizado para o atendimento de sua finalidade pública, conforme o interesse público, com o objetivo de executar competências legais e de cumprir as atribuições legais do serviço público.

Art. 11. As OM do COMAER devem adotar mecanismos para que os titulares de dados pessoais usufruam dos direitos assegurados pela LGPD e normativos correlatos.

Art. 12. O tratamento de dados pessoais sensíveis deve ocorrer somente nos termos da seção II do capítulo II da LGPD e são estabelecidos procedimentos de segurança no tratamento destes dados conforme orientações da LGPD e demais normativos.

Art. 13. O tratamento de dados pessoais de crianças e de adolescentes deve ser realizado nos termos da seção III do capítulo II da LGPD, bem como, pode ser realizado com base nas hipóteses legais previstas no art. 7º ou no art. 11 da mesma lei, desde que observado e prevalecente o seu melhor interesse, a ser avaliado no caso concreto, nos termos do art. 14 da Lei.

Art. 14. O uso compartilhado de dados pessoais deve ocorrer em estrita observância ao art. 26 da LGPD.

Parágrafo único. As operações remanescentes de uso compartilhado de dados devem seguir o disposto no Art. 27 da LGPD.

Art. 15. A transferência internacional de dados pessoais deve observar o disposto no Capítulo V da LGPD.

CAPÍTULO VI
CONSCIENTIZAÇÃO, CAPACITAÇÃO E SENSIBILIZAÇÃO

Art. 16. Os militares, servidores civis e demais colaboradores do COMAER, com acesso a dados pessoais devem participar de programas de conscientização, capacitação e sensibilização em matérias de privacidade e proteção de dados pessoais, objetivando adequar o tema aos seus papeis e responsabilidades.

CAPÍTULO VII
SEGURANÇA E BOAS PRÁTICAS

Art. 17. Considerando a necessidade de mitigar incidentes com dados pessoais, devem ser adotadas as seguintes medidas técnicas e organizacionais de privacidade e proteção de dados:

I - o acesso aos dados pessoais deve estar limitado as pessoas que realizam o tratamento;

II - as funções e responsabilidades dos colaboradores envolvidos nos tratamentos de dados pessoais devem ser claramente estabelecidas e comunicadas;

III - devem ser estabelecidos acordos de confidencialidade, termos de responsabilidade ou termos de sigilo com operadores de dados pessoais; e

IV - todos os dados pessoais devem estar armazenados em ambiente seguro, de modo que terceiros não autorizados não possam acessá-los.

Art. 18. Qualquer ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos dados pessoais dos titulares deve ser comunicada a Autoridade Nacional de Proteção de Dados (ANPD) dentro do prazo previsto pela LGPD.

Art. 19. A Estrutura de Governança de Proteção de Dados Pessoais do COMAER deve manter uma base de conhecimento com documentos que apresentam condutas e recomendações que melhoram o gerenciamento de risco e orientam na tomada de decisões adequadas em casos de comprometimento de dados pessoais.

CAPÍTULO VIII
AUDITORIA E CONFORMIDADE

Art. 20. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de privacidade e proteção de dados pessoais e da garantia das cláusulas de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 21. As atividades, produtos e serviços desenvolvidos no COMAER devem observar os requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes para estarem em conformidade.

Art. 22. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

CAPÍTULO IX
FUNÇÕES E RESPONSABILIDADES

Art. 23. Qualquer pessoa natural ou jurídica de direito público ou privado que tenha interação em qualquer fase do tratamento de dados pessoais deve assegurar a privacidade e a proteção de dados pessoais que trata, mesmo após o término do tratamento, observando as medidas técnicas e administrativas determinadas pela Estrutura de Governança de Proteção de Dados Pessoais do COMAER.

Art. 24. Compete ao Comitê de Governança Digital, de Segurança da Informação e de Proteção de Dados (CGDSIPD), com apoio da Estrutura de Governança de Proteção de Dados Pessoais do COMAER:

I - promover a proteção de dados pessoais e a adequação do COMAER à LGPD;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre proteção de dados pessoais;

III - participar da elaboração da Política de Proteção de Dados Pessoais e das demais normas internas de privacidade e proteção de dados pessoais, além de propor atualizações e alterações nestes dispositivos;

IV - a responsabilidade por gerenciar a implementação da LGPD dentro da organização e a administração da Política de Proteção de Dados Pessoais; e

V - incentivar a conscientização, capacitação e sensibilização das pessoas que desempenham qualquer atividade de tratamento de dados pessoais dentro do COMAER.

Art. 25. A constituição e a dinâmica de funcionamento do CGDSIPD serão definidas por Portaria do Comandante da Aeronáutica.

Art. 26. A responsabilidade pelas decisões relacionadas ao tratamento de dados pessoais é do CMTAER, que no exercício das atribuições típicas de controlador determina as medidas necessárias para executar a Política de Proteção de Dados Pessoais dentro de sua estrutura organizacional.

Art. 27. Compete ao Controlador do COMAER:

I - observar os fundamentos, princípios da privacidade e proteção de dados pessoais e os deveres impostos pela LGPD e por normativos correlatos no momento de decidir sobre um futuro tratamento ou realizá-lo;

II - considerar o preconizado pelos art. 7º, art. 11 e art. 23 antes de realizar o tratamento de dados pessoais;

III - cumprir o previsto pelos art. 46 e art. 50 da LGPD buscando à proteção de dados pessoais e sua governança;

IV - indicar um encarregado pelo tratamento de dados pessoais, divulgando a identidade e as informações de contato do encarregado de forma clara e objetiva, preferencialmente no sítio institucional;

V - elaborar o inventário de dados pessoais a fim de manter registros das operações de tratamento de dados pessoais;

VI - reter dados pessoais somente pelo período necessário para o cumprimento da hipótese legal e finalidade utilizadas como justificativa para o tratamento de dados pessoais;

VII - criar e manter atualizados os avisos ou políticas de privacidade, que informarão sobre os tratamentos de dados pessoais realizados em cada ambiente físico ou virtual, e como os dados pessoais neles tratados são protegidos; e

VIII - requerer do titular a ciência com o termo de uso para cada serviço ofertado, informatizado ou não, que trate dados pessoais.

Art. 28. É vedado qualquer tratamento de dados pessoais para fins não relacionados com as atividades desenvolvidas pela organização ou por pessoa não autorizada formalmente pelo COMAER.

Art. 29. São considerados operadores de dados pessoais as pessoas naturais ou jurídicas de direito público ou privado, que realizam operações de tratamento de dados pessoais em nome do controlador.

Parágrafo único. Quaisquer fornecedores de produtos ou serviços, que por algum motivo, realizam o tratamento de dados pessoais a eles confiados, são considerados operadores e devem seguir as diretrizes estabelecidas nesta política.

Art. 30. Compete aos Operadores de dados pessoais para o COMAER:

I - observar os princípios estabelecidos no art. 6º da LGPD, ao realizar tratamento de dados pessoais;

II - seguir as diretrizes estabelecidas pelo controlador; e

III - antes de efetuar o tratamento, verificar se as diretrizes estabelecidas pelo controlador cumprem os requisitos legais presentes nos art. 7º, art. 11 e art. 23 da LGPD;

Parágrafo único. Não é competência do operador decidir unilateralmente quanto aos meios e finalidades utilizados para o tratamento de dados pessoais.

Art. 31. Compete ao Encarregado de proteção de dados do COMAER:

I - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações e requisições da ANPD e adotar providências;

III - orientar os colaboradores da organização a respeito das práticas a serem adotadas em relação à proteção de dados pessoais; e

IV - executar as demais atribuições determinadas pelo agente de tratamento ou estabelecidas em normas complementares.

Art. 32. Ao receber comunicações da ANPD, o encarregado adotará as medidas necessárias para o atendimento da solicitação e para o fornecimento de informações pertinentes, adotando, dentre outras, as seguintes providências:

I - encaminhar internamente a demanda para as unidades competentes

II - fornecer orientação e a assistência necessárias ao agente de tratamento; e

III - indicar expressamente o representante do agente de tratamento perante a ANPD para fins de atuação em processos administrativos, quando esta função não for exercida pelo próprio encarregado.

Art. 33. O encarregado de proteção de dados prestará assistência e orientação ao agente de tratamento na elaboração, definição, e implementação de:

I - registro e comunicação de incidente de segurança;

II - registro das operações de tratamento de dados pessoais;

III - relatório de impacto à proteção de dados pessoais;

IV - mecanismos internos de supervisão e de mitigação de riscos relativos ao tratamento de dados pessoais;

V - medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

VI - processos e políticas internas que assegurem o cumprimento da LGPD, e dos regulamentos e orientações da ANPD;

VII - instrumentos contratuais que disciplinem questões relacionadas ao tratamento de dados pessoais;

VIII - transferências internacionais de dados;

IX - regras de boas práticas e de governança e de programa de governança em privacidade, nos termos do art. 50 da LGPD;

X - produtos e serviços que adotem padrões de design compatíveis com os princípios previstos na LGPD, incluindo a privacidade por padrão e a limitação da coleta de dados pessoais ao mínimo necessário para a realização de suas finalidades; e

XI - outras atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais.

Art. 34. Compete ao agente de tratamento:

I - prover os meios necessários para o exercício das atribuições do encarregado, neles compreendidos, entre outros, recursos humanos, técnicos e administrativos;

II - solicitar assistência e orientação do encarregado quando da realização de atividades e tomada de decisões estratégicas referentes ao tratamento de dados pessoais;

III - garantir ao encarregado a autonomia técnica necessária para cumprir suas atividades, livre de interferências indevidas, especialmente na orientação a respeito das práticas a serem tomadas em relação à proteção de dados pessoais;

IV - assegurar aos titulares meios céleres, eficazes e adequados para viabilizar a comunicação com o encarregado e o exercício de direitos; e

V - garantir ao encarregado acesso direto às pessoas de maior nível hierárquico dentro da organização, aos responsáveis pela tomada de decisões estratégicas que afetem ou envolvam o tratamento de dados pessoais, bem como às demais áreas da organização.

CAPÍTULO X
CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 35. Os contratos, convênios, acordos e instrumentos similares atualmente em vigor, que de alguma forma envolvam o tratamento de dados pessoais, precisam incorporar cláusulas específicas em total conformidade com a presente Política de Proteção de Dados Pessoais e que contemplem minimamente:

I - requisitos mínimos de segurança da informação.;

II - determinação de que o operador não processe os dados pessoais para finalidades que divergem da finalidade principal informada pelo controlador;

III - requisitos de proteção de dados pessoais que os operadores de dados pessoais devem atender;

IV - condições sob as quais o operador deve devolver ou descartar com segurança os dados pessoais após a conclusão do serviço, rescisão de qualquer contrato ou de outra forma mediante solicitação do controlador; e

V - diretrizes especificas sobre o uso de subcontratados pelo operador para execução contratual que envolva tratamento de dados pessoais.

Art. 36. As OM do COMAER devem adotar medidas rigorosas com o propósito de assegurar que os terceiros e processadores de dados pessoais contratados estejam plenamente em conformidade com as cláusulas contratuais estabelecidas no momento da celebração do acordo entre as partes envolvidas.

CAPÍTULO XI
PENALIDADES

Art. 37. Ações que violem a Política de Proteção de Dados Pessoais poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Art. 38. Casos de descumprimento desta Política serão registrados e comunicados ao Encarregado de Tratamento de Dados do COMAER para ciência e tomada das providências cabíveis.

ANEXO XXV
POLÍTICA DE ACESSIBILIDADE DIGITAL

CAPÍTULO XII
PROPÓSITO

Art. 1º Esta Política tem como propósito a adoção de tecnologias pelas organizações públicas federais e outros entes jurisdicionados ao Tribunal de Contas da União (TCU) que permitam ao público PCD (pessoas com deficiência) acessar sítios e serviços públicos digitais

Art. 2º A Acessibilidade Digital refere-se ao desenvolvimento e ao design de tecnologias, websites, aplicativos e conteúdos digitais de maneira que possam ser utilizados por todas as pessoas, independentemente de suas habilidades físicas, sensoriais, cognitivas ou tecnológicas. O objetivo principal é eliminar barreiras que possam dificultar o acesso ou a interação de pessoas com deficiência ou outras limitações, como dificuldades temporárias ou restrições técnicas, além de contextualizar a organização no compromisso com a inclusão digital e o cumprimento de normas e padrões.

Art. 3º Esta Política de Acessibilidade Digital foi elaborada incluindo os seguintes pontos principais:

I - alinhamento com normas e diretrizes:

a) implementar as recomendações do eMAG (Modelo de Acessibilidade em Governo Eletrônico), que estabelece padrões para acessibilidade digital no Brasil e está alinhado ao WCAG do W3C, padrão internacional para acessibilidade na web.

II - recursos e ferramentas de acessibilidade:

a) garantir funcionalidades como ajuste de contraste, atalhos de navegação por teclado (Alt + número) e ferramentas de busca acessíveis para pessoas com deficiência.

III - infraestrutura física e digital:

a) Promover a inclusão de rampas, banheiros adaptados e outros elementos de acessibilidade nos espaços físicos da FAB; e

b) nos portais e sistemas digitais, implementar práticas de acessibilidade como legendas em vídeos e compatibilidade com leitores de tela.

IV - transparência e participação:

a) estimular a abertura de dados acessíveis por meio do Portal Brasileiro de Dados Abertos, garantindo clareza, periodicidade e granularidade na disponibilização das informações.

V - treinamento e conscientização:

a) promover capacitações para o efetivo uso e manutenção de recursos acessíveis por parte de servidores e fornecedores, reforçando o compromisso com a inclusão.

VI - monitoramento e melhoria contínua:

a) realizar auditorias periódicas de acessibilidade para identificar e corrigir falhas, promovendo a melhoria contínua dos serviços e espaços.

Art. 4º Essas ações fortalecem o compromisso do COMAER com a inclusão e garantem o cumprimento das normas legais e regulamentares aplicáveis, como os decretos federais sobre acessibilidade e o direito ao acesso à informação.

Seção I
Das diretrizes gerais

Art. 5º As diretrizes estabelecem o escopo de aplicação desta Política, priorizando áreas críticas de atendimento e serviços, e definem os níveis de conformidade necessários para garantir que as plataformas digitais do COMAER permaneçam alinhadas aos mais altos padrões de acessibilidade e eficiência.

Subseção I
Escopo

Art. 6º Esta Política de Acessibilidade Digital aplica-se a todo o conteúdo digital disponibilizado nos sites e sistemas do COMAER.

Parágrafo único. A implementação ficará a cargo dos Elos do STI responsáveis pelos serviços Web.

Subseção II
Dos padrões de referência

Art. 7º Esta Política adota as **Web Content Accessibility Guidelines** (WCAG) como referência global, juntamente com o Modelo de Acessibilidade em Governo Eletrônico (eMAG), que oferece adaptações específicas para o contexto brasileiro, garantindo que as diretrizes permaneçam alinhadas às necessidades locais e internacionais de acessibilidade.

Subseção III
Do nível de conformidade

Art. 8º Fica estabelecido como meta o cumprimento do nível AA das Diretrizes de Acessibilidade para Conteúdo da Web (WCAG) e o atendimento integral às diretrizes do Modelo de Acessibilidade em Governo Eletrônico (eMAG), com o objetivo de assegurar a acessibilidade dos serviços digitais fornecidos à sociedade.

Subseção IV
Do nível de maturidade

Art. 9º O COMAER busca alcançar um nível intermediário de maturidade em acessibilidade digital, alinhado às diretrizes da Cartilha de Boas Práticas para Acessibilidade Digital na Contratação de Desenvolvimento Web.

Parágrafo único. Esse objetivo envolve a adoção dos critérios WCAG 2.1 (nível AA), a inclusão da acessibilidade em todas as etapas do desenvolvimento, a capacitação de equipes, o monitoramento contínuo e a evolução para uma cultura organizacional inclusiva. Dessa forma, a organização visa oferecer sistemas e serviços digitais acessíveis, robustos e alinhados aos princípios de inclusão, reafirmando seu compromisso com a acessibilidade no setor público.

Seção II
Das funções e responsabilidades

Art. 10. A implementação e supervisão da acessibilidade digital será realizada pelo Elo Especializado do STI responsável por Acessibilidade Digital, com especialistas em acessibilidade previstos na Cartilha de Boas Práticas para Acessibilidade Digital na Contratação de Desenvolvimento Web.

Seção III
Da preparação de conteúdo

Art. 11. O Órgão Central do STI deve estabelecer processos que assegurem a criação de todo novo conteúdo em conformidade com as diretrizes de acessibilidade, abrangendo textos, imagens, vídeos e documentos, de forma a garantir a inclusão e a usabilidade para todos os usuários.

Seção IV
Da garantia de qualidade

Art. 12. O Elo Especializado responsável deve conduzir auditorias regulares em sites e sistemas digitais para avaliar a conformidade com as diretrizes de acessibilidade estabelecidas, identificando e corrigindo eventuais falhas de forma contínua e proativa.

Seção V
Da infraestrutura

Art. 13. É função do Órgão Operador das Soluções de TI garantir que os sistemas de gestão de conteúdo (CMS) e outras ferramentas digitais sejam compatíveis com os padrões de acessibilidade.

Seção VI
Dos relatórios e monitoramento

Art. 14. Cabe ao Elo Especializado responsável por Acessibilidade Digital elaborar e encaminhar ao Órgão Central do STI para revisão e publicação, relatórios anuais que detalhem os progressos alcançados em acessibilidade digital, apresentando métricas de conformidade com as diretrizes estabelecidas e incorporando o feedback dos usuários, a fim de promover transparência e melhorias contínuas nos serviços digitais.

ANEXO XXVI
TERMO DE RESPONSABILIDADE DA POLÍTICA DE CONTROLE DE ACESSO

COMANDO DA AERONÁUTICA
[Nome da OM].

TERMO DE RESPONSABILIDADE

Pelo presente instrumento, eu _____ (nome completo), SARAM/CPF nº _____, lotado(a) na Organização Militar _____, DECLARO , sob pena das sanções cabíveis previstas na Lei 8.112/1990, Decreto-lei nº 1.002, de 21 de outubro de 1969 e Decreto nº 76.322, de 22 de setembro de 1975, que assumo a responsabilidade por:

I - tratar o(s) ativo(s) de informação como patrimônio do COMAER;

II - utilizar as informações em qualquer suporte sob minha custódia, exclusivamente, no interesse do serviço do COMAER;

III - contribuir para assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações, conforme descrito na Instrução Normativa nº 01, do Gabinete de Segurança Institucional da Presidência da República, de 27 de maio de 2020, que Dispõe sobre Estrutura de Gestão de Segurança da Informação nos órgãos e nas entidades da administração pública federal;

IV - utilizar as credenciais, as contas de acesso e os ativos de informação em conformidade com a legislação vigente e normas específicas do STI;

V - responder, perante o COMAER, pelo uso indevido das minhas credenciais ou contas de acesso e dos ativos de informação;

VI - acessar a rede corporativa, computadores, Internet e/ou utilização de **e-mail**, somente com autorização (usuário/senha), por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de **e-mail**;

VII - utilizar o correio eletrônico (**e-mail**) colocado a minha disposição somente por necessidade de serviço ou por determinação expressa de superior hierárquico, realizando as tarefas e operações, em estrita observância aos procedimentos, normas e disposições contidas na Resolução Normativa que rege o acesso à rede corporativa, computadores, Internet e/ou utilização de **e-mail**;

VIII - não revelar, fora do âmbito profissional, fato ou informação de qualquer natureza de que tenha conhecimento por força de minhas atribuições, salvo em decorrência de decisão competente na esfera legal ou judicial, bem como de autoridade superior;

IX - manter a necessária cautela quando da exibição de dados em tela, impressora ou na gravação em meios eletrônicos, a fim de evitar que deles venham a tomar ciência pessoas não autorizadas;

X - não me ausentar da estação de trabalho sem encerrar a sessão de uso do navegador (**browser**), bloquear estação de trabalho, bem como encerrar a seção do cliente de correio, garantindo assim a impossibilidade de acesso indevido por terceiros;

XI - não revelar minha senha de acesso à rede corporativa, computadores, Internet e/ou do correio eletrônico (**e-mail**) a ninguém e tomar o máximo de cuidado para que ela permaneça somente de meu conhecimento; e

XII - responder em todas as instâncias, pelas consequências das ações ou omissões de minha parte que possam pôr em risco ou comprometer a exclusividade de conhecimento de minha senha ou das transações a que tenha acesso.

Local, UF, _____ de _____de_____.

_____

Assinatura

Nome do usuário e seu setor organizacional

_____

Nome da autoridade responsável pela autorização do acesso

AVISO DE PRIVACIDADE

O Comando da Aeronáutica coletará e tratará seus dados de acordo com a Lei 13.709 de agosto de 2018 (LGPD), com a **finalidade** de ceder acesso aos seus militares possuidores de larga experiência profissional e reconhecida competência técnico-administrativa, **limitando-se ao mínimo de dados** para a realização da contratação do referido serviço. Os dados **não serão compartilhados** por terceiros e nem utilizados fora da finalidade da coleta. **Os dados pessoais coletados ficarão constante em nossa base de dados e ao fim da vigência, as informações serão tratadas conforme o previsto nas leis arquivísticas vigentes.**

O requerente ao serviço, titular dos dados pessoais, concorda com o tratamento de seus dados pessoais para a finalidade determinada de forma livre e inequívoca.

ANEXO XXVII
TERMO DE EXCEÇÃO PARA USO DE SOFTWARE SEM SUPORTE

1) Solicitante:

OM/Setor:

Nome do Solicitante:

2) Identificação do **software**:

Nome do **Software**:

Versão:

Fabricante:

Data de Expiração do Suporte:

3) Justificativa para exceção

Descreva a razão pela qual o **software** sem suporte é considerado necessário para o cumprimento da missão da organização. Especifique os processos ou operações que dependem do **software** e as consequências de sua descontinuação ou substituição.

4) Controles de mitigação que serão adotados:

Liste os controles técnicos, operacionais ou administrativos que foram implementados para mitigar os riscos associados ao uso do **software** sem suporte. Estes controles podem incluir, mas não estão limitados a, monitoramento adicional, uso de **firewalls**, restrição de acesso, **backups** frequentes, entre outros.

5) Prazo estimado para o uso da exceção:

Ex: 180 dias.

6) Avaliação de riscos à segurança da informação:

Devem ser apresentados o riscos residuais, aqueles remanescentes mesmo após a implementação de controles de mitigação. O solicitante e a área responsável pela TI devem reconhecer e aceitar o risco associado ao uso do **software** sem suporte.

7) Aceitação do Risco Residual:

Eu, abaixo assinado, aceito o risco residual associado ao uso do **software** descrito acima, compreendendo as implicações para a segurança da informação e a continuidade das operações da organização.

_____ _____

Nome do Solicitante Chefe do Elo do STI apoiador

Local, ___/___/_____.

Aprovação pelo Órgão Central do STI:

A Diretoria de Tecnologia da Informação da Aeronáutica (DTI) revisou o pedido de exceção e, após avaliação dos controles de mitigação e riscos residuais, decide que a solicitação de exceção solicitada foi:

[ ] Autorizada

[ ] Negada

Comentários Adicionais Órgão Central do STI (quando necessários):

_____

<Posto e Nome do Diretor de Tecnologia da Informação da Aeronáutica>
Diretor de Tecnologia da Informação da Aeronáutica

Local, ___/___/____.

ANEXO XXVIII
TERMO DE AUTORIZAÇÃO PARA LIMPEZA REMOTA DE DADOS EM DISPOSITIVOS PORTÁTEIS

1)OM/Setor Solicitante

OM:

Setor:

2)Proprietário/Portador do Dispositivo

OM:

Setor:

Nome do Militar/Servidor:

3)Objetivo

O presente Termo de Autorização tem como objetivo obter o consentimento do militar/civil assemelhado para que o COMAER possa realizar a limpeza remota de dados corporativos armazenados em dispositivos portáteis de sua propriedade ou fornecidos pela organização, em conformidade com as políticas internas de segurança da informação.

4)Circunstâncias para Limpeza Remota

A limpeza remota de dados poderá ser realizada nas seguintes circunstâncias:

- Em caso de perda ou roubo do dispositivo portátil.
- Em caso de desligamento do militar/civil assemelhado da organização.

Sempre que o dispositivo estiver comprometido de forma a representar um risco à segurança dos dados corporativos.

Em outras situações em que o STI julgar apropriado para proteger as informações corporativas, conforme as políticas de segurança vigentes.

5)Dispositivos Abrangidos

Este termo abrange qualquer dispositivo portátil que o militar/civil assemelhado utilize para acessar ou armazenar dados corporativos, incluindo, mas não se limitando a:

- Smartphones.
- Tablets.
- Notebooks.

Dispositivos de armazenamento móvel (como discos rígidos externos e pen drives) conectados a redes ou sistemas da organização.

6)Direitos e Responsabilidades do militar

O militar/civil assemelhado autoriza expressamente o COMAER a realizar a limpeza remota de dados corporativos nos dispositivos descritos, em qualquer das circunstâncias mencionadas acima.

O militar/civil assemelhado compreende que a limpeza remota poderá resultar na perda permanente de dados armazenados no dispositivo, incluindo dados pessoais, se o dispositivo for de propriedade da organização.

O militar concorda em seguir as políticas de uso de tecnologia e de segurança da informação estabelecidas pela organização, garantindo que o dispositivo esteja configurado para permitir a limpeza remota.

Em caso de alteração na posse ou no uso do dispositivo (como transferência para outra pessoa ou uso não autorizado), o militar/civil assemelhado deve notificar imediatamente o STI.

7)Declaração de Consentimento

Eu, abaixo assinado, declaro que li e compreendi todas as disposições deste Termo de Autorização. Estou ciente e de acordo com os procedimentos descritos, autorizando o COMAER a tomar medidas, incluindo a limpeza remota de dados, para proteger as informações corporativas armazenadas nos dispositivos portáteis que utilizo.

_____

Nome do Militar/Servidor

Local, ___/___/_____.