MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO

PORTARIA DTI/GOVS Nº 171, DE 24 DE JUNHO DE 2025

Protocolo COMAER nº 67131.001303/2025-91

Aprova a Instrução que dispõe sobre o Uso das Redes de Dados no COMAER (Intraer e Internet).

O **DIRETOR DE TECNOLOGIA DA INFORMAÇÃO DA AERONÁUTICA**, no uso das atribuições que lhe conferem o art. 5º da Portaria n° 634/GC3, de 11 de dezembro de 2023, e o art. 6º do Regulamento da Diretoria de Tecnologia da Informação da Aeronáutica, aprovado pela Portaria n° 905/GC3, de 04 de fevereiro de 2025, resolve:

Art. 1º Aprovar a Instrução (ICA 7-63), na forma dos anexos I, II, III, IV, V, VI, VII, VIII, IX, X, XI, para o Uso das Redes de Dados no COMAER (Intraer e Internet).

Art. 2º Revoga-se a Portaria DTI Nº103/SNOR, de 15 de maio de 2024 ICA 7-61 Uso das Redes de Dados no Comaer (Intraer E Internet).

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

TECNOLOGIA DA INFORMAÇÃO

ICA 7–61

USO DAS REDES DE DADOS NO COMANDO DA AERONÁUTICA (INTRAER E INTERNET)

2025

ANEXO I
USO DAS REDES DE DADOS NO COMANDO DA AERONÁUTICA (INTRAER E INTERNET) (ICA 7–61)

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Seção I
Finalidade

Art. 4º A presente Instrução tem por finalidade regular e doutrinar os critérios, os procedimentos, os níveis adequados de segurança da informação e as atribuições para uso da Rede de Dados Intraer/Internet no Comando da Aeronáutica.

Seção II
Conceituações

Art. 5º Para os fins desta Portaria, serão adotadas as seguintes conceituações:

I - COMAER: Comando da Aeronáutica;

II - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;

III - acesso remoto: consiste na capacidade de um computador acessar, à distância, um outro computador ou de uma rede de computadores e, assim, visualizar arquivos, o **desktop** e até controlar programas e as funcionalidades dos dispositivos acessados;

IV - acesso seguro: combinação de processos ou soluções de segurança projetados para impedir o acesso não autorizado aos ativos digitais de uma organização e a perda de dados confidenciais;

V - acesso à Intraer: 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;

VI - AP: é um dispositivo que permite que dispositivos sem fio se conectem a uma rede local, servindo como uma ponte entre a rede com fio e dispositivos como **notebooks**, **smartphones** e **tablets**, transmitindo dados por meio de sinal Wi-Fi;

VII - aplicativo: trata-se de um **software** para computadores e/ou aparelhos móveis, que permite o desempenho de uma tarefa específica para usuários finais;

VIII - ataque cibernético: tentativas não autorizadas de explorar, roubar e/ou causar danos a informações confidenciais aproveitando-se de sistemas de computador vulneráveis. Visam causar danos ou obter o controle ou o acesso a documentos e sistemas importantes em uma rede de computadores pessoais ou comerciais;

IX - ativos da informação: patrimônio composto de bases de dados e arquivos, documentação de sistemas, informações sobre pesquisas, manuais de usuários, material de treinamento, procedimentos de suporte e operação, planos de continuidade, procedimentos de recuperação de sistemas, trilhas de auditoria e informações armazenadas;

X - ativos de **software**: patrimônio composto de aplicativos, sistemas operacionais, ferramentas de desenvolvimento e utilitários;

XI - ativos de tecnologia da informação: são todos os itens, físicos ou virtuais, que compõem a infraestrutura de TI. Ou seja, todo **hardware**, **software**, redes e outras tecnologias fundamentais para a continuidade das operações;

XII - ativos físicos: patrimônio da Instituição, composto de equipamentos computacionais (ex: processadores, monitores, **laptops**, modems), equipamentos de comunicação (ex: roteadores, **switchs**, **hubs**, PABX, aparelhos de **fac-símile**, secretárias eletrônicas), mídias removíveis (ex: fitas, discos rígidos, **pendrives**) e outros recursos tecnológicos (ex: impressoras, **nobreaks**, estabilizadores);

XIII - autenticação: processo de verificação da identidade de um objeto ou uma pessoa;

XIV - autenticidade: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;

XV - canalização de dados: infraestrutura de telecomunicações utilizada para o tráfego de dados, voz e imagem;

XVI - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizada e credenciada;

XVII - código fonte: conjunto de arquivos de texto contendo todas as instruções que devem ser executadas, expressas de forma ordenada numa linguagem de programação;

XVIII - **datacenters**: local físico que armazena máquinas de computação e seus equipamentos de **hardware** relacionados. contém a infraestrutura de computação que os sistemas de TI exigem, como servidores, unidades de armazenamento de dados e equipamentos de rede;

XIX - disponibilidade: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade. (Instrução Normativa GSI/PR no 1, de 13 de junho de 2008);

XX - DNS: define como os nomes de domínio são encontrados e traduzidos no endereço de protocolo da Internet. Um nome de domínio é um recurso fácil de ser lembrado quando referenciado como um endereço na Internet;

XXI - domínio: é o nome de identificação único de um **site** na Intraer/Internet, por exemplo, ".Intraer" ou "fab.mil.br". Ele é formado pelo nome e pela extensão: "fab" é o nome do domínio e o ".mil.br" é a extensão;

XXII - **e-mail** (mensagem eletrônica): documento digital produzido ou recebido via sistema de correio eletrônico, incluindo ou não, anexos que possam ser transmitidos junto à mensagem;

XXIII - Elo Especializado do STI: são aqueles que, por atribuições regimentais ou por terem sido instituídos em ato específico, executam atividades ou serviços especializados de TI de interesse do COMAER;

XXIV - Elos de Coordenação do STI: são os setores pertencentes aos Órgãos de Direção-Geral, de Direção Setorial (ODGS) e aos Órgãos de Assistência Direta e Imediata ao Comandante da Aeronáutica, responsáveis pela coordenação de suas atividades de TI junto ao Órgão Central do STI;

XXV - Elos de Serviço do STI: são os setores de TI das OM do COMAER que executam atividades rotineiras de manutenção de TI, reportando-se aos seus respectivos Elos de Coordenação;

XXVI - endereços IP: protocolo de Internet ou **Internet Protocol** (IP) que permite a comunicação entre dispositivos na rede. De forma genérica, pode ser considerado como um conjunto de caracteres que representa o local de um determinado equipamento em uma rede privada ou pública;

XXVII - estações de trabalho (**workstations**): computadores direcionados a atividades profissionais que, frequentemente, demandam bastante desempenho no processamento de dados;

XXVIII - **hacker**: indivíduo que elabora e modifica **software** ou **hardware** de computadores, seja desenvolvendo funcionalidades novas, seja adaptando as antigas. O termo é usado, na maioria das vezes, para se referir a programadores maliciosos que violam, de modo ilegal ou imoral, sistemas de tecnologia da informação, causando danos;

XXIX - **hiperlink**, páginas **web** e portal:

a) **hiperlink** é trecho contido em uma página **web** que direciona para outra página, sítio (**site**) ou para outro local da mesma página. Esse trecho pode estar contido em um texto, botão ou imagem;

b) página **web** é qualquer documento que faça parte de um sítio **web** e que costuma conter ligações (**links**) para facilitar a navegação entre os conteúdos; e

c) portal é uma plataforma **web** que agrega informações de diferentes fontes em uma única interface, apresentando as informações mais relevantes para cada usuário de acordo com seu contexto.

XXX - homologado: aquilo que foi desenvolvido, acompanhado e implantado por intermédio de processo ou procedimento estabelecido pelo STI e aceito pelo demandante;

XXXI - HT: Hotel de Trânsito;

XXXII - implantação: significa desenvolver um plano, introduzir ou estabelecer uma novidade, iniciar algo novo;

XXXIII - implementação: significa ação de pôr em prática um plano, entrada em vigor de acordo, assegurar a realização ou executar algo;

XXXIV - incidentes de segurança da informação: um evento ou uma série de eventos indesejados ou inesperados que podem vir a comprometer a confidencialidade, a integridade ou a disponibilidade de ativos físicos, de **software** ou de informação, todos de interesse da instituição;

XXXV - infraestrutura de telecomunicações: instalação planejada com o objetivo de conectar, interligar e fornecer suporte a toda a rede de comunicação da maneira mais adequada para o ambiente corporativo;

XXXVI - infraestrutura de TI: refere-se aos componentes necessários para executar e gerenciar ambientes de TI empresarial. Esses componentes incluem **hardware**, **software**, rede, sistema operacional e armazenamento de dados;

XXXVII - integridade: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XXXVIII - LAN: redes de Área Local ou **Local Area Network** (LAN) interligam computadores presentes dentro de um mesmo espaço físico, permitindo a troca de informações e recursos entre os dispositivos participantes;

XXXIX - LDAP: é um protocolo de aplicação aberto, livre de fornecedor e padrão de indústria para acessar e manter serviços de informação de diretório distribuído sobre uma rede;

XL - **lobby**: forma de comunicar, debater ou tentar convencer parlamentares ou executivos do governo (além de funcionários próximos, como assessores e secretários) a tomar uma decisão para atender a interesses particulares ou gerais;

XLI - **logout**: conjunto de procedimentos para desconectar um usuário de um computador, de um servidor ou de outro recurso da rede;

XLII - MAN: Rede de Área Metropolitana ou **Metropolitan Area Network** (MAN) conecta diferentes redes dentro de um raio de dezenas de quilômetros. Esse tipo de rede interliga computadores e usuários de unidades de uma empresa por meio de conexão pública (**link** de Internet);

XLIII - mensagem instantânea: forma de comunicação que acontece via Internet, por meio de um aplicativo ou **software**, com o objetivo de oferecer o diálogo em tempo real entre seus usuários;

XLIV - NAT: **Network Address Translation**;

XLV - NTP: é um protocolo para sincronização dos relógios dos computadores baseado no protocolo UDP utilizado para sincronização do relógio de um conjunto de computadores e dispositivos em redes de dados com latência variável;

XLVI - OM: Organização Militar;

XLVII - Órgão Central do STI: a Portaria nº 549/GC3, de 09 de agosto de 2010, reformulou o Sistema de Tecnologia da Informação do COMAER e designou a Diretoria de Tecnologia da Informação da Aeronáutica (DTI) como Órgão Central do STI;

XLVIII - programa: conjunto de instruções que descrevem uma tarefa a ser realizada por um computador. O termo refere-se ao código-fonte, escrito em alguma linguagem de programação, ou ao arquivo que contém a forma executável deste código-fonte.do STI;

XLIX - programas irregulares: **softwares** não padronizados pelo Órgão Central;

L - programas regulares: **softwares** padronizados pelo Órgão Central do STI;

LI - protocolos de acesso remoto: conjunto de regras para comunicação entre computadores que permite que usuários tenham acesso às suas respectivas áreas de trabalho sem estar fisicamente próximos a seus computadores. Exemplos de protocolos: RDP (**Remote Desktop Protocol**), VNC (**Virtual Network Computing**), SSH (**Secure Shell**);

LII - provedores de acesso à Intraer: o provedor de Internet, ou **Internet Service Provider** (ISP), é o intermediador que faz com que a Internet chegue até os dispositivos. É um serviço promovido por empresas especializadas, que oferecem Internet banda larga com conexões via cabo, satélite, rádio ou fibra;

LIII - WAN: uma rede de longa distância ou **Wide Area Network** (WAN) é uma rede de telecomunicações privada, geograficamente distribuída, que interconecta várias redes locais (LANs);

LIV - redes sociais: **sites** e aplicativos usados por pessoas e organizações que se conectam com clientes, familiares, amigos e pessoas que compartilham interesses em comum;

LV - renovação do certificado: processo de modificar a emissão e instalação do Certificado Digital de pessoa física ou jurídica;

LVI - servidor de rede: computador que oferece um serviço ou que compartilha com outros computadores em uma rede, recursos na forma de arquivos, impressoras, etc.;

LVII - sistema: conjunto integrado de componentes regularmente inter-relacionados e interdependentes criados para realizar um objetivo definido, com relações definidas e mantidas entre seus componentes, cuja operação como um todo é melhor que a soma de suas partes;

LVIII - sistema operacional: conjunto de programas que gerenciam recursos, processadores, armazenamento, dispositivos de entrada e saída, e dados da máquina e seus periféricos;

LIX - sistema operacional homologado: garantia de que o sistema operacional desenvolvido ou adquirido atende aos requisitos do negócio e está dentro dos padrões de qualidade e desempenho desejados;

LX - sistemas irregulares: sistemas que não passaram pelo processo de homologação no STI;

LXI - sistemas regulares: sistemas que passaram pelo processo de homologação no STI;

LXII - SNMP: é um protocolo utilizado para monitorar e gerenciar dispositivos de rede, como roteadores, **switches** e servidores, permitindo a coleta de informações sobre o desempenho, falhas e status desses dispositivos em tempo real;

LXIII - **software**: trata-se de um serviço computacional utilizado para realizar ações nos sistemas de computadores. Ou seja, um **software** é todo programa presente nos diversos dispositivos (computadores, celulares, televisores, entre outros);

LXIV - **software** cliente: refere-se ao **software** que atua do lado do dispositivo cliente, buscando como seu destino o **software** do lado do servidor de rede;

LXV - soluções de TI: não se define apenas como um único recurso. É, basicamente, todo o conjunto de sistemas, **softwares**, equipamentos, máquinas, ferramentas e quaisquer aplicações utilizadas para dar suporte aos projetos e processos do dia a dia, com o objetivo de torná-los mais eficientes e enxutos;

LXVI - SSID: é o nome que identifica uma rede sem fio, permitindo que dispositivos localizem e se conectem a ela. É exibido como o nome da rede Wi-Fi nas listas de redes disponíveis e pode ser configurado para ser visível ou oculto;

LXVII - subdomínio: subdomínio é um endereço que faz parte do domínio, ou seja, é uma ramificação que faz referência a uma parte de um domínio na Intraer/Internet. Exemplo: Na Intraer: Para o endereço http://www.dti.Intraer. Nesse caso, o domínio é Intraer e o sub-domínio é "DTI";

LXVIII - sítios de bate-papo: espaço virtual na Internet que reúne pessoas, geralmente identificadas por apelidos (**nicknames**), para trocar, em tempo real, mensagens escritas sobre os mais diversos assuntos;

LXIX - termo de compromisso e de manutenção de sigilo: documento firmado entre duas ou mais partes com o objetivo de manter determinadas informações em sigilo;

LXX - trabalho remoto/ teletrabalho: prática dos funcionários de realizarem suas tarefas em um local que não o escritório central operado pelo empregador;

LXXI - usuário: são pessoas que fazem uso de um determinado tipo de serviço, objeto, dispositivo ou produto;

LXXII - VLAN: **Virtual Local Area Network**;

LXXIII - VPN: conexão de rede privada entre dispositivos através da Internet. Utilizadas para transmitir dados de forma segura e anônima em redes públicas; e

LXXIV - WPS: é um padrão de segurança criado para simplificar o processo de conexão de dispositivos a uma rede Wi-Fi, permitindo que dispositivos sejam conectados ao **Access Point** (AP) de forma fácil, sem precisar inserir manualmente uma senha.

Seção I
Âmbito

Art. 6º Esta Instrução se aplica a todas às Organizações do COMAER.

CAPÍTULO II
INTRAER

Seção I
Da estrutura da rede

Art. 7º A Intraer é composta pela integração das redes locais (LAN) das Organizações do COMAER, por meio de infraestrutura de telecomunicações.

Art. 8º Nas diversas localidades do Brasil, existem organizações militares (OM) do COMAER que possuem uma infraestrutura de telecomunicação denominada Rede Metropolitana (MAN) que interliga as redes locais das OM existentes no Brasil.

Art. 9º Dessa forma, todas as Redes Metropolitanas estão interligadas, em nível nacional, constituindo uma Rede de Longa Distância (WAN).

Art. 10º Os Elos de Serviço que concentram os serviços de TI de uma guarnição e os Elos Especializados são considerados provedores de acesso à Intraer.

Seção II
Das soluções de TI que utilizam recursos da Intraer

Art. 11º A utilização e o consumo da Intraer como infraestrutura de comunicação de dados para suporte ao tráfego de informações oriundas ou destinadas a sistemas ou a aplicativos, desenvolvidos ou adquiridos por iniciativa própria ou por aquisição em processo licitatório, estão sujeitos aos seguintes fatores condicionantes, conforme estabelecido no Anexo XI:

I - o projeto da solução de TI deve ser submetido ao Órgão Central do STI, para análise e aprovação, com antecedência mínima de 90 dias em relação à data prevista para a sua entrada em operação;

II - o processo de implantação da solução de TI deve ser acompanhado por representantes do Órgão Central do STI;

III - a solução de TI deve ser submetida a testes de comunicação, acompanhados por representantes do Órgão Central do STI, que comprovem sua capacidade de operar nas condições técnicas disponíveis na Intraer;

IV - a entrada em operação do aplicativo só deverá ocorrer com autorização expressa do Órgão Central do STI;

V - a implantação de soluções de TI, cujo consumo de recursos de rede esteja limitado à rede local da OM interessada, poderá ser processada, desde que preenchidos os requisitos deste artigo e que a solução de TI não venha a sobrecarregar a rede da OM, prejudicando de forma acentuada o acesso a soluções de TI de interesse do COMAER que são operadas naquela OM;

VI - a suspensão do suporte da Intraer a uma solução de TI pode ocorrer, a qualquer tempo, em caráter temporário ou permanente, caso a solução de TI em questão passe a comprometer o desempenho da Intraer e, principalmente, a adequada operacionalidade de sistemas de interesse do COMAER;

VII - a depender da complexidade do sistema e disponibilização de meios para análise de segurança cibernética (e.g. ambiente de teste), o Órgão Central do STI poderá solicitar um novo prazo para aprovação; e

VIII - fica vedada a instalação de sistemas ou aplicativos na infraestrutura de TI da Intraer das OM se a forma de acesso ocorrer pela Internet. Caso o acesso do sistema ou aplicativo seja realizado pela Internet, a OM deverá proceder conforme estabelecido nesta Instrução.

Seção III
Acessos remotos à rede local de uma OM

Art. 12º O acesso remoto à rede local de uma OM permite o acesso a serviços como servidores de arquivos, administração de servidores, administração de ativos físicos, etc. Tais serviços não estão disponíveis para o acesso remoto à rede Intraer por intermédio de VPN.

Art. 13. A solicitação de acesso remoto à rede local de uma OM deve ser aprovada pelo respectivo Elo de Coordenação do STI e pelo Órgão Central do STI, conforme Processo de Acesso Remoto às Redes que Compõem a Intraer (Anexo VIII).

Art. 14. O pedido de acesso à rede local de uma OM deve ser solicitado, exclusivamente, pela equipe técnica do Elo de Serviço para realização de manutenções e ou intervenções na infraestrutura de TI.

Art. 15. Esse pedido de acesso, também, poderá ser solicitado para as situações em que as empresas terceirizadas precisem realizar manutenções e atualizações nos ativos de TI na infraestrutura de TI da Intraer, via Internet, para serviços adquiridos através de contratações. Vale destacar que as empresas contratadas devem assinar o Termo de Compromisso e de manutenção de sigilo e respeito às normas de segurança vigentes no COMAER, a ser assinado pelo representante legal da contratada, conforme orientado em normas vigentes.

Art. 16. Os Centros de Computação deverão disponibilizar serviços de acesso remoto à infraestrutura de TI da Intraer através da Internet, conforme determinações do Órgão Central do STI.

Art. 17. Todo acesso remoto à rede Intraer deverá ser realizado pelos servidores de rede hospedados nos datacenters dos Centros de computação da FAB.

Art. 18. Os Centros de computação deverão estabelecer critérios para o acesso seguro e monitorar os acessos à rede Intraer via Internet.

Art. 19. O acesso remoto à rede local de uma OM, por meio da Internet, deve ser feito por meio da combinação da VPN com outros protocolos, como: SSH, RDP, VNC, ETC.

Art. 20. O acesso remoto à rede local de uma OM, por meio da Internet, é estritamente pessoal e intransferível, com validade de 12 meses.

Seção IV
Acesso remoto à rede Intraer por intermédio de VPN

Subseção I
Da aplicação

Art. 21. Todo acesso remoto à rede Intraer deverá ser realizado pelos servidores de rede hospedados nos datacenters dos Elos de Serviço e dos Elos Especializados do STI.

Art. 22. O pedido de acesso à rede Intraer por intermédio da VPN deve ser solicitado pelo usuário ou Elo de serviço para o trabalho remoto a fim de acessar os sistemas homologados pelo STI disponibilizados na Intraer, tais como: SIGADAER, SILOMS, Portal da OM, Página **web** hospedadas no domínio Intraer, dentre outros.

Subseção II
Da instalação

Parágrafo único. Para atender aos requisitos de instalação do acesso seguro, é obrigatório que o sistema operacional da estação de trabalho esteja homologado e atualizado, bem como possua um **software** de antivírus em iguais condições.

Subseção III
Da solicitação da VPN

Art. 23. Esse serviço deverá ser solicitado ao Comandante/Chefe/Diretor da OM pelo chefe imediato do militar/civil, conforme disposto na NSCA 7-13 Norma de Sistema que Dispõe Sobre a segurança da Informação e Defesa Cibernética nas Organizações do Comando da Aeronáutica.

Art. 24. As solicitações de acessos à VPN aprovadas deverão ser encaminhadas pela OM ao Elo Especializado, via SAU.

Art. 25. O Chamado do SAU deverá conter uma cópia do Termo de Responsabilidade devidamente preenchido e assinado.

Art. 26. Elo Especializado deverá manter atualizada a lista de usuários das OM cujos os acessos à VPN estejam sob sua responsabilidade.

Art. 27. O Termo de Responsabilidade poderá ser assinado digitalmente ou fisicamente, sendo mandatório o mesmo padrão de assinatura por todos no documento, inclusive pela autoridade responsável pela solicitação.

Art. 28. Os arquivos do sistema de acesso seguro serão enviados via e-mail corporativo FAB "fab.mil.br" ao usuário e a senha para acesso será enviada via **e-mail** pessoal cadastrado no Portal do Militar (Portal de Pessoal/Dados pessoais/cadastro/contatos/Endereço Eletrônico).

Subseção IV
Do acesso seguro

Art. 29. O acesso seguro à Intraer, por meio da Internet, é estritamente pessoal e intransferível, com validade de 12 meses.

Art. 30. As solicitações de novos acessos serão realizadas conforme disposto nesta Instrução.

Art. 31. A autenticação para utilização do acesso seguro deverá utilizar as credenciais do **Login** Único.

Art. 32. A interrupção do acesso seguro poderá ocorrer a qualquer tempo por motivo de segurança ou por expiração do acesso.

Art. 33. As renovações dos acessos VPN serão processadas de forma automatizada, pelo Elo Especializado responsável, desde que o usuário conste na lista atualizada de sua OM.

Art. 34. As OM interessadas em manter os acessos à VPN deverão encaminhar anualmente ao Órgão Central do STI, via Ofício, sua lista atualizada dos usuários autorizados a ter seu acesso renovado.

Art. 35. A renovação do certificado para o acesso seguro será enviada para o e-mail corporativo FAB "fab.mil.br" do usuário com as seguintes informações:

I - expiração do acesso;

II - novo prazo de validade para a renovação do acesso;

III - portal de acesso para o **download** dos arquivos e tutoriais necessários para acesso à VPN;

IV - código de acesso para **download** dos arquivos (enviado para o **e-mail** particular cadastrado no Portal do Militar); e

V - orientações para o processo de instalação e utilização do acesso VPN.

Art. 36. Por medida de segurança e com o intuito de conter possível ataque cibernético, os acessos seguros que permanecerem inativos por 60 (sessenta) dias consecutivos poderão ter o fornecimento do serviço interrompido pelos Elos Especializados.

Art. 37. O acesso seguro é realizado com autenticação de senha, mediante utilização de cliente VPN específico instalado na estação de trabalho de cada usuário.

Art. 38. É terminantemente proibido aos usuários a alteração do código-fonte do cliente VPN.

Art. 39. Também é terminantemente proibido, por razões de segurança da Intraer, acessar a Intraer e a Internet simultaneamente nos equipamentos cujo Cliente VPN foi configurado, sob pena de sanções administrativas e legais.

Seção V
Do compartilhamento de recursos da Intraer com outras redes

Art. 40. O compartilhamento de recursos (servidores de rede, estações de trabalho, ativos de TI, etc.) utilizados na Intraer com a Internet ou outras redes só poderá ocorrer com autorização expressa do Órgão Central do STI.

Art. 41. A solicitação para compartilhamento desses recursos deverá ser encaminhada pela OM interessada ao Órgão Central do STI, via seu Elo de Coordenação do STI, com antecedência mínima de 180 dias.

Art. 42. A solicitação de compartilhamento de recursos da Intraer com outras redes deverá seguir o modelo/desenho conforme estabelecido no Processo de Solicitação de Compartilhamento de Recursos entre a Intraer e Outras Redes (Anexo X).

Seção VI
Dos endereços IP e DNS

Art. 43. A atribuição e controle dos endereços IP é de responsabilidade do Centro de Gerenciamento Técnico do Sistema de Controle do Espaço Aéreo Brasileiro - CGTEC, conforme estabelecido na ICA 66-32 "Núcleo de Gerenciamento Técnico do SISCEAB - NUCGTEC".

Art. 44. A atribuição e o controle dos registros de DNS é de responsabilidade do Órgão Central do STI.

Art. 45. O padrão de nome de domínio a ser utilizado pela Organização é a sequência de letras minúsculas e algarismos correspondentes à sigla da OM, sem qualquer sinal gráfico (hífen, travessão, barra, espaço, sinais de pontuação, acentos gráficos, etc.), seguidos da expressão "Intraer", como, por exemplo:

I - bagl.Intraer;
II - comar1.Intraer;
III - pamals.Intraer; e
IV - srpvmn.Intraer.

Art. 46. As estruturas sistêmicas do COMAER utilizarão o padrão de domínio letras minúsculas correspondestes à sigla do Sistema, sem qualquer sinal gráfico (hífen, travessão, barra, espaço, sinais de pontuação, acentos gráficos, etc.), seguidos da expressão "Intraer", como, por exemplo: sti.Intraer.

Seção III
Do acesso ao domínio Intraer

Art. 47. Todo usuário da Intraer no COMAER deverá assinar um Termo de Responsabilidade e de Conhecimento da Política de Segurança da Informação (POSIN) do COMAER e das Políticas de Segurança da Informação Definidas pelas Respectivas Organizações (Anexo II).

Art. 48. O acesso ao domínio será exclusivamente realizado por ativos de TI pertencentes ao patrimônio do COMAER. Esses equipamentos devem ser configurados pelos Elos de serviço ou especializado do STI, devendo ser inseridos no subdomínio "OM" do domínio "Intraer".

Art. 49. As contas de acesso à rede estão vinculadas à infraestrutura de TI da OM apoiadora em que o usuário está lotado. Cada conta de acesso à rede corresponde a uma única conta de autenticação na rede Intraer.

Art. 50. A conta de acesso à rede protege o acesso a qualquer dado que tramite pela Intraer. Essa conta deve ser criada logo que o usuário se apresenta na OM e deve ser excluída no momento de seu desligamento.

Art. 51. A conta de acesso à rede é acessada por **login** e senha, com validade de 2 anos, e somente poderá ser utilizada pelo usuário cadastrado. A senha é pessoal e intransferível não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Ficam vedados os acessos múltiplos simultâneos, como também os funcionais que não identifiquem o usuário.

Art. 52. Para a Intraer, a formação da conta de acesso à rede deve ser uma sequência de letra minúsculas que identifique o nome-de-guerra e as iniciais do nome completo do militar (no caso de civis, o nome pelo qual é conhecido o funcionário), por exemplo:

I - Maj. Av. Marco Aurélio da SILVA ⟶ silvamas.

Art. 53. Para os casos em que o usuário possua o mesmo nome de guerra e as iniciais para formação de sua conta, deve se proceder da seguinte maneira:

a) 1° Ten Av. Marco Aurélio da SILVA ⟶ silvamas.
b) Maj Av Maurício Albuquerque de SILVA ⟶ silvamas1.

Art. 54. Deve ser adicionado um numeral em sequência no final das iniciais da conta, levando em prioridade o momento da confecção. No caso apresentado como exemplo, a conta do Major foi confeccionada posteriormente à conta do Tenente.

CAPÍTULO III
INTERNET

Seção I
Acesso funcional das OM do COMAER à Internet

Art. 55. As organizações do COMAER deverão acessar à Internet por meio dos acessos regionais autorizados pelo Órgão Central do STI.

Art. 56. Eventualmente, o Órgão Central do STI poderá autorizar a implantação, em caráter provisório, de acessos à Internet em OM do COMAER, distintos dos acessos regionais, podendo a OM solicitante contratar serviço comercial de provedor da localidade, desde que instale em sua rede local os equipamentos de segurança estabelecidos pelo STI para a conexão com a Internet. Se os equipamentos de segurança forem adquiridos pela própria OM, as especificações, as configurações, as conexões e a montagem devem ser aprovadas pelo Órgão Central do STI, antes de se tornar operacional a conexão com a Internet.

Art. 57. O acesso à Internet de caráter provisório será concedido nos casos de exercício ou operação militar conforme estabelecido no MCA 400-24 - Manual da Unidade Celular de Tecnologia da Informação - UCTI.

Art. 58. A solicitação de autorização para implantação, em OM do COMAER, de acessos provisórios à Internet deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à implantação do acesso, a submeterá ao Órgão Central do STI, conforme estabelecido no Processo de Solicitação de Acessos Provisórios à Internet (Anexo IX).

Art. 59. Os recursos para manutenção do acesso provisório e para os equipamentos utilizados na solução de segurança implementada são de responsabilidade da OM onde será implantado o ponto de acesso àquela rede.

Art. 60. Todo acesso à Internet deve ser utilizado pelo usuário cadastrado via **login** e senha. A senha é pessoal e intransferível, não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Fica vedado os acessos múltiplos, como também os funcionais que não identifiquem os usuários.

Art. 61. O usuário para possuir o acesso à Internet, com validade de 2 anos, deverá solicitar através do Sistema de Atendimento ao Usuário (SAU), mediante assinatura de termo de responsabilidade, conforme estabelecido no Termo de Responsabilidade para Uso de Internet e Mídias Sociais (Anexo III).

Art. 62. Todo usuário da Internet no COMAER deverá assinar um Termo de Responsabilidade e de Conhecimento da Política de Segurança da Informação (POSIN) do COMAER e das Políticas de Segurança da Informação Definidas pelas Respectivas Organizações (Anexo II).

Art. 63. Todo o tráfego de dados com acesso à Internet deve ser protegido por ferramentas contra **malware**.

Art. 64. O Órgão Central do STI é responsável pela padronização e fornecimento do **software** de antivírus corporativo.

Art. 65. As OM poderão adquirir **software** de antivírus distintos do padronizado, desde que autorizado pelo respectivo Elo de Coordenação do STI e pelo Órgão Central do STI, e com os recursos previstos no planejamento financeiro da respectiva OM e que seja integrado aos sistemas de monitoramento de vulnerabilidades padronizado no COMAER e gerenciado pelo Centro de Tratamento de Incidentes de Redes da Força Aérea Brasileira (CTIR.FAB).

Art. 66. A utilização do acesso à Internet está restrita ao atendimento das necessidades de serviço da Organização do COMAER.

Art. 67. As Organizações do COMAER detentoras de acessos provisórios à Internet deverão monitorar o seu uso pelo pessoal devidamente autorizado, mediante credencial de segurança (ICA 200-13), e habilitado, providenciando para que sejam corrigidas as discrepâncias observadas.

Art. 68. O monitoramento do acesso provisório à Internet deverá também ser realizado pelos Elos Especializados, sendo responsabilidade da OM disponibilizar acesso à solução de segurança.

Seção II
Das soluções de TI na Internet

Art. 67 A entrada em operação de soluções de TI, cujo acesso será feito a partir da Internet, só poderá ser efetivada quando autorizada por meio de documento oficial emitido pelo Órgão Central do STI.

Art. 69. A solicitação de autorização para entrada em operação de soluções de TI disponibilizados na Internet deverá ser feita pela Organização interessada ao seu respectivo Elo de Coordenação do STI que, caso seja de parecer favorável à entrada em operação do sistema, a submeterá ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação e quanto às necessidades de canalização de dados. conforme estabelecido no Anexo V.

Art. 70. As soluções de TI disponibilizadas na Internet deverão ser, obrigatoriamente, hospedados nos equipamentos servidores de rede dos Centros de Computação da Aeronáutica.

Art. 71. A realização de ajustes, determinados pelo Órgão Central do STI, nas soluções de TI disponibilizadas na Internet, será de responsabilidade da OM interessada, mediante acompanhamento e coordenação dos Elos Especializados regionais.

Seção III
Dos acessos não funcionais à Internet

Subseção I
Da concentração regional de TI

Art. 72. Com a reestruturação do COMAER houve necessidade de criação e desativação de OM, nesse sentido, houve a exclusão de alguns Grupamentos de Apoio - GAP e as suas infraestruturas de TI passaram a ser responsabilidades das novas OM. Dessa forma, a concentração de serviços de TI nos GAP conforme preconizado no Força Aérea 100 foi modificada e, atualmente, existem concentração de serviços em GAP/Bases/OM de Ensino.

Art. 73. Com a implementação da Concentração dos Serviços de Tecnologia da Informação, conforme previsto no MCA 11-2, enlaces de comunicação de alta velocidade foram concentrados em algumas OM para acesso à Internet, os quais foram providos com ferramentas de proteção de perímetro com capacidade de mitigar riscos associados à Segurança Cibernética, de modo a atender às regulamentações em vigor.

Art. 74. No processo de concentração de TI, identificou-se a necessidade de padronizar os acessos não funcionais das Organizações Militares do COMAER, com vistas a também adequá-los às legislações de TI vigentes no âmbito do Governo Federal, tais como o armazenamento de registros de acesso previstos pelo § 1°, 5° e 6° do Art. 13 da Lei nº 12.965 de 22 de abril de 2014 (Marco Civil da Internet), transcrito no item a seguir.

Subseção II
Das situações autorizadas para acesso

Art. 75. Os procedimentos gerais para o acesso não funcional à Internet provido por Organização Militar do COMAER devem ser aplicáveis as seguintes situações:

I - acesso à Internet provido por Hotéis de Trânsito (cabeado ou Wi-Fi);

II - acesso Wi-Fi à Internet em Elo de Serviço do STI;

III - acesso Wi-Fi à Internet em Exercício ou Operação; e

IV - qualquer tipo de ponto de acesso contratado e mantido por Organização da Aeronáutica.

Seção IV
Da implantação e uso de rede sem fio (Wireless)

Art. 76. O processo de configuração de uma rede sem fio deve seguir rigorosamente as orientações de segurança previstas por esta Instrução, garantindo a conformidade com as etapas de implementação detalhadas.

Art. 77. Para assegurar a proteção adequada da rede sem fio e implementar os controles essenciais de segurança da informação, é indispensável o uso de equipamentos que estejam de acordo com as especificações descritas nesta Instrução.

Art. 78. Devem ser considerados os seguintes requisitos mínimos de **hardware**:

I - o **Access Point** (AP) deve ser compatível com padrões 802.11ac ou superiores;

II - é mandatório que os equipamentos suportem o protocolo WPA2 ou superior;

III - o AP deverá possibilitar atualizações de **firmware**, a fim de incorporar novos padrões e eventuais correções de segurança lançadas pelo fabricante;

IV - o AP deverá ter as configurações padrão alteradas, tais como senhas, SSID, chaves e SNMP **communities**; e

V - os equipamentos de rede deverão ser capazes de realizar a geração de eventos de segurança, mediante a criação de **logs** de eventos.

Art. 79. Para o gerenciamento de serviços locais e remotos por meio do protocolo **Simple Network Management Protocol** (SNMP) deverão ser considerados os aspectos a seguir:

a) o nome da **community** SNMP para **read** no agente do AP deve ser de difícil dedução, evitando o uso do nome padrão "**public**", para impedir acessos não autorizados às configurações do dispositivo;

b) o nome da **community** SNMP para **write** escrita no agente do AP deve ser de difícil dedução, evitando o uso do nome padrão "**private**", visando impedir alterações não autorizadas nas configurações do dispositivo; e

c) o acesso de **read-write** SNMP ao agente do AP deve ser removido, sendo concedido apenas quando estritamente necessário.

Art. 80. Os protocolos de configuração (HTTP, SNMP, telnet, etc.) que não serão utilizados para o gerenciamento devem ser desabilitados, optando, sempre que possível, pelo gerenciamento do AP por meio de rede cabeada ou via conexão serial, minimizando as possibilidades de conexão e configuração inadvertida do AP por meio de um cliente **wireless**.

Art. 81. Caso a funcionalidade esteja disponível, é recomendada a aplicação da filtragem baseada em endereços físicos (MAC **address**).

Art. 82. Os administradores de rede deverão verificar regularmente a existência de novos **patches**, **upgrades** ou atualizações junto aos fornecedores, testá-los previamente e, após a garantia de correto funcionamento, aplicá-los.

Art. 83. A versão do **firmware** do AP deve ser atualizada para a última versão estável disponível, corrigindo falhas de segurança que podem comprometer a disponibilidade ou a segurança do dispositivo.

Art. 84. A função Wi-Fi **Protected Setup** (WPS) dos dispositivos AP deverá ser desabilitada.

Art. 85. É essencial que haja uma diferenciação clara entre a padronização das redes sem fio de acesso funcional, ou seja, aquelas acessíveis a partir de dentro de uma OM, e as redes sem fio de acesso não funcional, como as usadas exclusivamente para conexão à Internet em locais como Hotéis de Trânsito (HT).

Subseção I
Da implantação de rede sem fio para acesso funcional

Art. 86. A rede sem fio para acesso funcional deve ser separada fisicamente ou logicamente da rede cabeada da OM por meio de uma DMZ ou VLAN, de forma a evitar que a rede interna seja diretamente acessada.

Art. 87. O equipamento de rede sem fio para acesso funcional não deve operar como uma ponte direta entre a rede sem fio e a rede cabeada.

Art. 88. Todas as conexões da rede sem fio para acesso funcional com outras redes externas, incluindo a Internet, devem ser protegidas por **firewalls**.

Art. 89. A rede sem fio para acesso funcional deve ser isolada por meio de **Virtual Local Area Network** (VLAN), permitindo a implementação de controles de acesso restritos que filtrem e autorizem somente o tráfego de protocolos e serviços previamente aprovados.

Art. 90. A potência de transmissão deve ser ajustada de forma que, sempre que possível, a cobertura eletromagnética não ultrapasse os limites físicos das instalações da OM. Portanto, deverão ser realizadas avaliações locais para determinar a posição ideal dos AP, garantindo a eficiência da cobertura e a segurança da rede.

Art. 91. O AP deverá, obrigatoriamente, oferecer suporte à utilização do protocolo SNMP v3, garantindo a implementação de recursos avançados de segurança, como autenticação e criptografia.

Art. 92. As OM devem considerar a segurança física como parte fundamental da arquitetura de rede **wireless**. Os equipamentos devem ser protegidos fisicamente para evitar violação ou roubo, e o acesso ao botão de reset dos AP, caso tenham, deve ser restringido para impedir o manuseio por pessoas não autorizadas.

Art. 93. É recomendável a instalação de câmeras de monitoramento que garantam a vigilância contínua dos pontos de acesso.

Art. 94. Os AP deverão ser configurados para impedir tráfego em horários fora do expediente.

Art. 95. O acesso à administração do AP deve ser restrito aos administradores da rede, usando ferramentas específicas, por exemplo, o **Captive Portal** do pfSense e/ou regras de **firewall**.

Art. 96. Deverão ser implantados mecanismos que ocultem ou protejam o esquema de endereçamento IP, configurando o **firewall** para bloquear escaneamentos de rede, utilizando **Network Address Translation** (NAT) e/ou segmentação da rede interna, de forma a impedir o acesso não autorizado e a visualização da arquitetura da rede.

Art. 97. Deverá ser implementado um mecanismo de autenticação na rede sem fio para acesso funcional, de modo a identificar a sessão por usuário. Para isso, deve-se utilizar métodos de autenticação via **Lightweight Directory Access Protocol** (LDAP) ou o uso de usuários e senhas pessoais e intransferíveis, permitindo a geração de registros de log e garantindo a execução de auditorias futuras.

Art. 98. É proibida a utilização de equipamentos de rede que não sejam de propriedade da OM.

Art. 99. É proibido o tráfego de dados contendo informações classificadas por meio de redes sem fio para acesso funcional, devendo ser utilizadas as redes e mecanismos institucionais adequados para essa finalidade, garantindo a segurança e a integridade das informações.

Art. 100. Deverá ser implementada uma política de uso formal a ser aceita pelo usuário no momento da conexão à rede sem fio para acesso funcional, utilizando ferramentas como o **Captive Portal** do pfSense ou soluções equivalentes. A política deve incluir, no mínimo, as seguintes diretrizes:

I - as credenciais de acesso à rede sem fio são pessoais e intransferíveis, e o usuário compromete-se a não compartilhá-las com terceiros;

II - o dispositivo utilizado para acessar a rede sem fio deve ser seguro, com o sistema operacional dentro do seu ciclo de vida;

III - o sistema operacional do dispositivo deve estar atualizado com todos os **patches** de segurança aplicados e com o antivírus devidamente configurado e atualizado;

IV - caso o dispositivo tenha um **firewall** disponível, este deve estar ativado e configurado corretamente para garantir a proteção contra acessos não autorizados; e

V - o usuário deve estar ciente de que todas as atividades realizadas na rede podem ser monitoradas e registradas, garantindo rastreabilidade e conformidade com auditorias futuras.

Art. 101. Deverá ser configurada corretamente a data e hora dos AP utilizando um servidor **Network Time Protocol** (NTP), garantindo precisão nos registros de eventos e permitindo auditorias com exatidão.

Art. 102. Deverá ser estabelecido um período de inatividade para o encerramento automático de sessões em máquinas conectadas à rede sem fio para acesso funcional, reduzindo o risco de uso indevido por atacantes ou usuários mal-intencionados com credenciais alheias.

Art. 103. Em virtude dos riscos inerentes ao uso da tecnologia de redes sem fio e a fim de preservar a segurança das informações do COMAER, não se recomenda a utilização de redes sem fio para acesso funcional à Intraer.

Art. 104. A decisão de implementar a rede sem fio para o uso da Intraer pode ocasionar riscos à Disponibilidade, Integridade, Confidencialidade e Autenticidade (DICA) de dados sensíveis nesta rede, tais como:

I - exposição a ataques de interceptação de sinal, facilitando a exfiltração de dados classificados por meio de **packet sniffing**;

II - aumento da vulnerabilidade a acessos não autorizados, devido à facilidade de captura do sinal da rede sem fio por agentes não autorizados em áreas de cobertura estendidas;

III - suscetibilidade a ataques de **man-in-the-middle** (MITM);

IV - possibilidade de comprometimento de dispositivos conectados à rede devido a falhas em protocolos de autenticação ou algoritmos de criptografia depreciados;

V - risco de comprometimento por meio de vulnerabilidades em equipamentos de rede sem fio, como explorações de falhas no **firmware** ou configurações inadequadas;

VI - suscetibilidade a ataques de **evil twin**, em que um AP malicioso é usado para enganar usuários e capturar credenciais; e

VII - potencial aumento de superfícies de ataque devido ao uso de dispositivos não gerenciados ou com níveis inadequados de **hardening** entre outros.

Art. 105. A despeito dos riscos elencados, caso o gestor da OM ainda assim decida pela implementação de uma rede sem fio para acesso funcional à Intraer, devem ser adotadas as medidas mais rigorosas de segurança, de modo a minimizar os riscos acima já expostos. Os critérios obrigatórios que devem ser implementados:

I - utilização de criptografia mais robusta, sendo WPA3 **only** o padrão mínimo aceitável, sendo vedado o uso de combinações WPA2 e WPA3 como, por exemplo, o modo **mixed**;

II - implementação de separação física e lógica das sub-redes que comporão o acesso à Internet e à Intraer, evitando o tráfego cruzado não autorizado;

III - utilização obrigatória da solução de antivírus padronizada pela DTI, garantindo que todos os dispositivos clientes conectados na rede estejam com agente do respectivo antivírus configurado;

IV - implementação de equipamentos de gerenciamento de tráfego, **firewall**, IDS/IPS (**Intrusion Detection and Prevention Systems**) para detectar e prevenir tentativas de intrusão e acessos não autorizados;

V - seja desabilitada a função DHCP e DNS no AP no momento da configuração inicial;

VI - atribuição de novos IPs na rede deverá ser feita por um **firewall** ou por servidor dedicado para esta funcionalidade na rede;

VII - não utilização de rede sem fio para acesso funcional à Intraer em dispositivos pessoais; e

VIII - cumprimento rigoroso de todas as determinações previstas nesta ICA sobre a implementação de redes sem fio, incluindo autenticação, controle de acesso, segmentação de tráfego e auditorias.

Art. 106. Caso o gestor da OM decida pela implementação de redes sem fio para acesso funcional à Intraer, considerando os riscos elencados, a OM será inteiramente responsável por mitigar

os riscos e arcar com eventuais consequências que comprometam a segurança da Intraer. Portanto, quaisquer danos causados por essa prática, como comprometimento da segurança, perda de confidencialidade ou falhas na integridade dos dados, serão de total responsabilidade da OM.

Subseção II
Da implantação de rede sem fio para acesso não funcional

Art. 107. A padronização dos acessos não funcionais das Organizações Militares do COMAER se faz necessária, com vistas a adequá-los às normas de segurança da informação e às diretrizes estabelecidas para redes sem fio.

Art. 108. O uso de redes Wi-Fi em instalações como HTs ou áreas administrativas, voltadas exclusivamente para o acesso à Internet, devem possuir requisitos distintos, sendo obrigatória a separação física e lógica das redes de acesso funcional.

Art. 109. As redes sem fio de acesso não funcional devem obedecer ao compêndio de regras e pré-requisitos estabelecidas nesta Instrução.

Art. 110. Todos os clientes da rede sem fio para acessos não funcionais deverão ser previamente identificados de forma personalíssima e intransferível, garantindo a rastreabilidade da conexão e o **compliance** com princípios de **non-repudiation**, visando possíveis auditorias futuras. As informações registradas devem permitir a identificação inequívoca do usuário e ser armazenadas sob sigilo, em ambiente controlado e de segurança, pelo prazo mínimo de 1 (um) ano, conforme previsto no Art. 13 da Lei nº 12.965/2014 (Marco Civil da Internet).

Art. 111. É obrigatório o conhecimento e o consentimento do Termo de Responsabilidade e de Conhecimento da Política de Segurança da Informação (POSIN) do COMAER e das Políticas de Segurança da Informação Definidas pelas Respectivas Organizações (Anexo II), para usuários da rede não pertencentes ao COMAER. O acesso à Internet será fornecido, mediante a assinatura do termo.

Art. 112. É recomendada a utilização de uma política de uso para todos os usuários da rede sem fio.

CAPÍTULO IV
INTERNET E INTRAER

Seção I
Da mensagem eletrônica

Art. 113. A mensagem eletrônica é um serviço de comunicação interna do COMAER, viabilizando as mensagens do tipo "**e-mail**". Este serviço pode ser acessado tanto pela Intraer (https://mail.Intraer/) quanto pela Internet (https://mail.fab.mil.br/).

Art. 114. Para o funcionamento do serviço de mensagem eletrônica do COMAER (FABMail), devem ser observadas as orientações dispostas na ICA 7-51.

Seção II
Das publicações de páginas na web
Subseção
Do conteúdo

Art. 115. O conteúdo das páginas **web** publicadas na Internet/Intraer são de responsabilidade do Comandante da OM. Deve ser observado que alguns assuntos, por motivos evidentes, não devem ser divulgados nessas páginas, como por exemplo:

I - planos ou Ordens referentes a operações militares;
II - referências que facilitem a obtenção de informações classificadas; e
III - informações de cunho pessoal sobre os militares e seus familiares.

Art. 116. Para a divulgação de informações em páginas **web** deve ser observado também o disposto no item 3.4.6 da RCA 205-47 "Regulamento para Salvaguarda de assuntos Sigilosos da Aeronáutica", de 7 de março de 2006.

Subseção II
Dos padrões

Art. 117. Além dos padrões já estabelecidos em legislação interna do COMAER, as páginas do COMAER na Internet/Intraer devem atender também aos Padrões Brasil e-Gov.

Seção III
Das páginas web

Art. 118. A página confeccionada será um template padronizado já existente e a OM irá editar e preencher com as respectivas informações.

Art. 119. Cabe às OM capacitarem o seu corpo técnico e administrativo na utilização da ferramenta implementada para criação da sua página **web**.

Subseção I
Das páginas na Intraer

Art. 120. A criação de páginas na **web** pelas OM da FAB é feita em parceria com o STI, seguindo etapas de confecção, registro de domínio e publicação, alinhadas às diretrizes institucionais:

I - confecção: as OM da FAB solicitarão ao Elo de Serviço do STI a criação da página, via SAL;
II - registro do domínio: as OM da FAB solicitarão ao órgão central do STI, via Ofício; e
III - publicação: a publicação será realizada pelo Elo de Serviço do STI em coordenação com a OM solicitante.

Subseção II
Das páginas na Internet

Art. 121. As Organizações do COMAER deverão utilizar subdomínios do domínio fab.mil.br para publicar suas páginas **web** na Internet.

Art. 122. Na eventualidade de surgirem condições especiais que requeiram o registro de domínios na Internet, fora do domínio fab.mil.br, estes só poderão ser efetivados quando autorizados, por meio de documento oficial emitido ao Órgão Central do STI, conforme estabelecido no Termo de Responsabilidade para Usuários da Rede Intraer (Anexo IV). Uma vez autorizados, o Órgão Central do STI efetuará o registro do domínio junto ao registro.br.

Art. 123. No que diz respeito à avaliação e necessidades da canalização de Internet, sempre que necessário, o Órgão Central do STI consultará o DECEA e solicitará o atendimento às demandas identificadas.

Art. 124. As páginas publicadas pelas Organizações do COMAER na Internet deverão ser, obrigatoriamente, hospedadas nos equipamentos servidores de rede dos Elos Especializados do STI.

Art. 125. Recomenda-se que o acesso às páginas **web** das Organizações do COMAER, publicadas na Internet seja realizado, a partir da página portal do COMAER na Internet (portal único do COMAER - https://www.fab.mil.br/organizacoes).

Art. 126. O processo de criação de páginas **web** deve atender aos padrões de uniformidade definidos pelo CECOMSAER, para isso as solicitações devem seguir as orientações estabelecidas no Anexo IV:

I - confecção: As OM da FAB solicitarão ao seu Elo de Coordenação do STI a criação da página. Após a aprovação destas pelo Elo de Coordenação do STI serão criadas pelo CCA-BR, mediante abertura de chamado SAU;

II - registro do domínio: O Elo de Coordenação do STI solicitará o registro do domínio ao Órgão Central do STI, via Ofício; e

III - publicação: Após aprovação do CECOMSAER, o Elo de Coordenação do STI solicitará a publicação da página ao CCA-BR, via SAU.

Seção IV
Das mídias sociais

Art. 127. A solicitação de autorização para publicação de perfis de mídia social corporativa deverá ser feita pela OM interessada ao seu respectivo Elo de Coordenação do STI.

Art. 128. O Elo de Coordenação do STI submeterá as solicitações aprovadas ao Órgão Central do STI, para avaliação quanto ao nível de segurança da informação, bem como ao CECOMSAER para a avaliação da identidade digital, recomendada pelo Governo Federal.

Art. 129. O conteúdo exposto nessas mídias é de inteira responsabilidade do Comandante/Chefe/Diretor da Organização Militar (OM).

Seção V
Das mensagem Instantânea

Art. 128 A solicitação de uso de serviços de mensagem instantânea, de sítios de bate-papo e de serviços associados às redes sociais é um procedimento que requer a devida auto- rização e definição de responsabilidades.

Art. 130. Esse serviço deverá ser solicitado ao Comandante/Chefe/Diretor da OM pelo chefe imediato do militar, conforme estabelecido no Termo de Responsabilidade para Uso de Internet e Mídias Sociais (Anexo III).

Art. 131. As solicitações de uso de serviços de mensagem instantânea aprovadas deverão ser encaminhadas ao Elo de Serviço do STI apoiador.

Art. 132. O Órgão Central do STI solicitará a coordenação dos Centros de Computação da Aeronáutica junto ao Elo de Serviço local para alinhar a execução das configurações necessárias na infraestrutura de TI no intuito de conceder o acesso.

Art. 133. Cabe ao Elo de Serviço realizar as configurações de acesso conforme orientações dos Centros de Computação.

CAPÍTULO V
RESTRIÇÕES RELATIVAS À SEGURANÇA DAS INFORMAÇÕES

Art. 134. É expressamente proibida a utilização dos recursos da Intraer/Internet nas seguintes situações:

I - atividades ilegais, fraudulentas e/ou maliciosas; político-partidárias; **lobby** ou proselitismo político ou religioso; propaganda de empresas ou instituições sem relação direta com a missão do COMAER; incitação à prática de crime ou de transgressão disciplinar;

II - causar prejuízos morais ou financeiros a terceiros;

III - explorar vulnerabilidades de outros sítios da Internet, promovendo ataques do tipo daqueles realizados por **hackers**;

IV - expressar discriminação, preconceito ou apologia ao vício ou ao emprego ou utilização de ações, procedimentos ou práticas consideradas ilegais ou contrários à moral e aos bons costumes;

V - realizar procedimentos que se configurem como crimes, tais como pirataria, pedofilia, assédio, difamação ou outros quaisquer que contrariem as leis em vigor ou a moral e os bons costumes;

VI - provocar danos à imagem do COMAER e das demais instituições governamentais;

VII - prejudicar a realização de atividades de interesse do COMAER;

VIII - atividades com o propósito de ganho pessoal ou comercial;

IX - uso de recursos computacionais com o propósito de acessar ou divulgar informação inapropriada, ofensiva ou contrária aos bons costumes;

X - armazenamento ou processamento de informação classificada, sem a devida autorização;

XI - obtenção, armazenamento, instalação e utilização de programas, sem o devido licenciamento junto à Empresa ou Instituição detentora legal dos seus direitos de uso;

XII - liberação do acesso, por parte de indivíduos não expressamente autorizados, de recursos disponíveis na Intraer, sejam estes recursos equipamentos, serviços de rede ou programas que foram licenciados para o COMAER;

XIII - atividades visando a modificação ou a substituição de programas padronizados pelo Órgão Central do STI para emprego nos servidores de rede ou nas estações de trabalho da Intraer;

XIV - atividades visando a modificação ou a substituição de programas aplicativos homologados e padronizados pelos Elos de Coordenação do STI, na sua área de responsabilidade, para emprego nos servidores de rede ou nas estações de trabalho da Intraer;

XV - atividades visando divulgar identidade dos usuários e senhas ou, de outro modo, permitir ou capacitar qualquer indivíduo não autorizado para acessar um sistema de TI do COMAER;

XVI - uso não autorizado de identificação ou senha individual;

XVII - atividades que permitam visualizar, modificar ou remover arquivos ou qualquer outro tipo de informação de propriedade de usuários da rede, sem a devida autorização;

XVIII - emprego de ferramentas que realizem análises nas redes locais (LAN), visando obter informações sobre os servidores de rede, as estações de trabalho clientes e os demais recursos das redes, exceto quando devidamente justificado e expressamente autorizado pelo Cmt/Chefe/Dir da OM, sob a supervisão do chefe do Elo de serviço que apoia a OM; e

XIX - emprego as redes metropolitanas e de longa distância, visando obter informações sobre os servidores de rede, as estações de trabalho clientes e os demais recursos das redes, exceto quando devidamente justificado e expressamente autorizado pelo Órgão Central do STI, via cadeia de comando, conforme estabelecido no Processo de Autorização para Uso de Ferramenta de Análise de Rede (Anexo VII).

CAPÍTULO VI
CONDIÇÕES GERAIS

Art. 135. Os usuários da Intraer devem estar cientes de que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos não requer consentimento para este monitoramento.

Art. 136. Os sistemas de informação e os dados que neles existem são bens do COMAER e devem ser protegidos contra a divulgação indevida e contra a perda de integridade, de disponibilidade e de confidencialidade.

Art. 137. Em particular, devem ser adotados adequadamente todos os procedimentos estabelecidos pelo Órgão Central do STI, quando necessário, devem ser adotadas medidas complementares, específicas de cada interessado, além daquelas preconizadas para uso geral ou recomendadas.

Art. 138. Em todos os níveis da rede, devem ser implementados os meios adequados de autenticação de usuários e de registro de suas atividades, de modo a possibilitar o conhecimento e a verificação de todas as ações realizadas. A autenticação e o registro são obrigatórios para qualquer que seja a modalidade de inicialização do sistema ou de acesso.

Art. 139. Vale destacar que a senha para qualquer acesso (Intraer/Internet) é pessoal e intransferível, não cabendo, em qualquer hipótese, a alegação de uso indevido após ato de compartilhamento. Fica vedado os acessos múltiplos, como também os funcionais que não identifiquem os usuários.

CAPÍTULO VII
COMPETÊNCIAS

Art. 140. Do Órgão Central do STI:

I - a supervisão técnica e operacional da Intraer;

II - o estabelecimento de normas para administração e uso da Intraer, inclusive para o planejamento, a aquisição, a manutenção, a utilização, a padronização, o controle de acesso, a segurança, o gerenciamento da rede e o treinamento dos operadores e dos usuários da Intraer;

III - avaliar, quanto ao nível de segurança das informações e quanto às necessidades de canalização de dados, as solicitações, encaminhadas pelos Elos de Coordenação do STI, relativas ao uso da Internet pelas OM do COMAER, que tratam da instalação de acessos provisórios, da publicação de páginas, da disponibilização de sistemas ou aplicativos e do acesso a sistemas de TI da Intraer;

IV - autorizar a entrada em operação de soluções de TI disponibilizados na Internet por OM do COMAER;

V - autorizar o acesso a sistemas de TI da Intraer a partir da Internet;

VI - dotar os Centros de Computação da Aeronáutica da infraestrutura de rede (equipamentos, programas e canalização de dados) necessária, bem como de níveis adequados de capacitação de pessoal, adequados ao funcionamento dos seus acessos à Intraer/Internet; e

VII - gerenciar o registro de domínios e subdomínios da Intraer/Internet para atender às Organizações do COMAER.

Art. 141. Dos Elos de Coordenação do STI:

I - analisar as solicitações encaminhadas pelas OM do COMAER, no contexto sob sua área de responsabilidade funcional, relativas ao uso da Internet, quando tratar de instalação de acessos

provisórios, da publicação de páginas, da disponibilização de soluções de TI, do acesso a sistemas de TI da Intraer e aquisição de **softwares** antivírus distintos do padronizado pelo Órgão Central do STI:

II - encaminhar as solicitações analisadas e consideradas adequadas ao Órgão Central do STI; e

III - fiscalizar, periodicamente, as páginas **web** já publicadas e aprovadas.

Art. 142. Do Elo Especializado do STI em Segurança da Informação:

I - compete a esse Elo, em coordenação com o Órgão Central do STI, orientar e controlar a utilização dos procedimentos de segurança da Intraer;

II - assessorar o Órgão Central do STI na avaliação de soluções técnicas de criptografia utilizadas para garantir a segurança das comunicações em acessos à Internet; e

III - produzir e disseminar conhecimentos acerca de incidentes de segurança da informação resolvidos e em andamento, objetivando prevenir ocorrências futuras.

Art. 143. Dos Demais Elos Especializados do STI:

I - operar os acessos à Internet sob sua responsabilidade garantindo os níveis de segurança da informação estabelecidos pelo Órgão Central do STI, bem como a disponibilidade dos acessos para atender às páginas **web** e aos sistemas aplicativos hospedados;

II - prover o CECOMSAER do apoio técnico necessário ao trato das suas competências referentes ao emprego da Internet;

III - gerar relatórios estatísticos relativos à utilização do acesso à Internet sob sua responsabilidade, por solicitação das Organizações do COMAER usuárias do acesso;

IV - apoiar os Elos de Serviço na resolução de incidentes de segurança da informação;

V - cooperarem com o Órgão Central do STI na operação e no controle de utilização da Intraer e, ainda, apoiar o funcionamento das redes locais das OM;

VI - configurar os servidores necessários aos acessos seguros cujo atendimento técnico for a eles atribuído pelo Órgão Central do STI;

VII - manter, por no mínimo 5 (cinco) anos, os registros dos acessos seguros distribuídos, para fins arquivísticos e legais, mantendo informações sobre a quantidade de acessos fornecidos por OM, os dados de identificação dos usuários que receberam os acessos, a data de início da disponibilização do acesso e há quanto tempo os acessos estão inativos;

VIII - deve possuir, para fins arquivísticos e legais, controle dos Termos de Responsabilidade, conforme estabelecido no Termo de Responsabilidade para Uso de Internet e Mídias Sociais (Anexo III), dos usuários que utilizam o acesso seguro por ele fornecido, por igual período; e

IX - prestar suporte técnico ao Elo de Serviço da OM, caso este não consiga solucionar a requisição ou o incidente reportado pelo usuário.

Art. 144. Do Elo de Serviço do STI:

I - prestar suporte técnico ao usuário, mediante abertura de chamado através do SAU;

II - cuidar para o contínuo funcionamento da rede local, por meio de inspeções periódicas;

III - supervisionar diariamente as operações da Intraer/Internet;

IV - cuidar da segurança local e cooperar com a segurança geral dos sistemas, instalações, equipamentos e redes que compõem a Intraer;

V - implementar, executar e controlar os procedimentos de segurança, incluindo a realização de cópias e a guarda adequada dos meios de recuperação dos sistemas;

VI - preservar a confidencialidade das informações disponíveis na rede local;

VII - controlar a concessão e a utilização de senhas, autenticações, contas, acessos e afins de interesse local para uso da Intraer/Internet;

VIII - providenciar para que o Comandante, Diretor ou Chefe da OM tome pronto conhecimento das irregularidades que observar no funcionamento da Intraer/Internet;

IX - controlar o acesso físico às instalações e aos equipamentos da Intraer de sua responsabilidade;

X - instalar somente programas e arquivos que tenham sido verificados previamente, quanto à existência de **softwares** maliciosos;

XI - inspecionar para que o equipamento não contenha **softwares** com licenças falsas e/ou programas que possam apresentar risco à rede Intraer, principalmente vírus, **worms**, **adware**, **spyware**, **ransomware**, **bot**, **rootkits**, cavalos de tróia e **bugs** conhecidos no código de **software** que possam comprometer a segurança da Intraer;

XII - cancelar os acessos aos sistemas de TI nos casos: transferência de OM ou reserva;

XIII - realizar abertura do chamado SAU sobre qualquer situação que enseje a perda ou a alteração da concessão para o uso do acesso seguro, conforme descrito nesta norma;

XIV - registrar a ocorrência de incidentes de segurança da informação, mediante SAU;

XV - a instalação do acesso VPN;

XVI - a instalação de programas obtidos da Internet é de responsabilidade da própria Organização, devendo respeitar as condições de licenciamento e suporte técnico a que o programa está submetido;

XVII - configurar os perfis de acesso definidos e controlar a manutenção dos requisitos para acesso às redes; e

XVIII - deve possuir, para fins arquivísticos e legais, controle dos Termos de Responsabilidade físicos assinados, Termo de Responsabilidade para Uso de Internet e Mídias Sociais (Anexo III) e Termo de Responsabilidade para Usuários da Rede Intraer (Anexo IV), dos usuários que utilizam o acesso Intraer e Internet por ele fornecido, por igual período.

Art. 145. Do CECOMSAER:

I - elaborar e manter atualizado o Portal da Força Aérea na Internet;

II - padronizar as informações de Comunicação Social da Aeronáutica divulgadas pela Internet;

III - fazer a triagem, selecionar e encaminhar às OM detentoras da informação solicitada as correspondências eletrônicas recebidas pela Internet e endereçadas ao Comando da Aeronáutica;

IV - responder as correspondências eletrônicas endereçadas ao Comandante da Aeronáutica;

V - analisar o conteúdo das propostas de páginas para a Internet apresentadas pelas OM do COMAER;

VI - as páginas para a Internet no COMAER serão consideradas propriedades digitais, devendo ser observado o disposto no Instrução Normativa SECOM-PR n° 8 de 19 de dezembro de 2014, com relação à adequação à identidade padrão de comunicação digital;

VII - as páginas para a Internet no COMAER necessitam observar o Manual de operação do Portal único da Força Aérea Brasileira; e

VIII - estabelecer conexão (**hiperlinks**) entre o Portal da Força Aérea e as páginas **web** cujas propostas tenham sido aprovadas pelo CECOMSAER.

Art. 146. Dos Comandantes, Chefes ou Diretores de OM:

I - viabilizar o uso adequado das redes de dados no âmbito da OM;

II - solicitar a criação das páginas **web** de sua OM;

III - cooperar com o STI com a manutenção e controle do funcionamento das redes de dados, disponibilizando equipe técnica para auxílio e atendimento quando lhe for solicitado subordinação sistêmica;

IV - implementar as medidas complementares de segurança física e lógica e as demais que forem necessárias para o adequado funcionamento da rede local e dos datacenters (principais concentradores da Intraer/Internet);

V - promover a capacitação de técnicos e de usuários de sistemas e soluções de TI do efetivo de sua OM;

VI - incluir na ficha de desimpedimento, um campo para certificação, pelo setor de Tecnologia da Informação, da efetivação de cancelamento, de remoção ou de encerramento de acessos, senhas, autorizações de acessos e afins, pertinentes ao pessoal movimentado da OM;

VII - impedir a instalação de programas ou de sistemas irregulares em computadores da Organização;

VIII - comunicar ao seu Elo de Coordenação do STI as irregularidades e/ou as sugestões relativas ao funcionamento da Intraer/Internet;

IX - assegurar que os equipamentos de TI da OM não contenham **softwares** com licenças falsas e/ou programas que possam apresentar risco à rede Intraer, principalmente **malwares** e **bugs** conhecidos no código de **software** que possam comprometer a segurança;

X - providenciar que o Elo de Serviço local realize abertura de chamado SAU para o cancelamento do acesso (acesso seguro por VPN, acesso remoto, acesso ao domínio Intraer) nos casos: mudança de função, transferência, missão, entre outros;

XI - informar prontamente via chamado SAU, qualquer situação que enseje a perda ou a alteração da concessão para o uso do acesso seguro, conforme descrito nesta norma; e

XII - concessão do acesso ao serviço de rede, cabendo ao responsável pela rede de TI local controlar a utilização delas.

Art. 147. Dos usuários:

I - manter sigilo e utilizar adequadamente senhas, autenticações, acessos, equipamentos, arquivos, programas e afins, para que não haja comprometimento nem da segurança, nem do funcionamento da Intraer/ Internet;

II - utilizar somente programas regularizados e de uso autorizado na Intraer;

III - realizar criteriosamente os procedimentos lógicos de **login** (conexão) e de **logout** (desconexão) da sua rede local;

IV - responder pela utilização das estações de trabalho, programas e arquivos sob sua responsabilidade;

V - cuidar da armazenagem apropriada das cópias de mensagens que devam ser preservadas;

VI - relatar qualquer irregularidade observada durante o uso da Intraer/Internet, a seu superior ou ao Administrador ou ao Gerente da rede local;

VII - verificar a autenticidade das mensagens de correio eletrônico sempre que julgar conveniente, na dúvida consulta o Elo de serviço do STI;

VIII - para os casos de furto, roubo, extravio dos equipamentos com acesso seguro VPN implica imediata notificação através do SAU;

IX - realizar abertura de chamado SAU para o fornecimento dos acessos aos sistemas de TI; e

X - realizar a boa utilização de programas instalados nas máquinas funcionais da Organização. Havendo necessidade de programas adicionais, o usuário deverá acionar a Elo de serviço local, via SAU.

CAPÍTULO VIII
INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Art. 148. Os incidentes de segurança da informação devem ser reportados tão logo sejam observados pelo Elo do STI ao Sistema de Atendimento ao Usuário (SAU), ou ao STI (DTI - Diretoria de Tecnologia da Informação da Aeronáutica/CTIR - Centro de Tratamento de Incidentes de Rede).

Art. 149. O Elo que reportar o incidente deverá preservar, tanto quanto possível, as evidências do incidente observado, conforme orientações a serem dadas pelo Órgão Central do STI, visando a possibilitar procedimentos específicos de análise ligados ao fato, a fim de garantir a legitimidade do procedimento e das evidências coletadas.

Art. 150. O atendimento aos incidentes de segurança da informação caberá a um dos Elos Especializados, conforme orientações do Órgão Central do STI, o qual coordenará, operacionalmente, a estrutura do CTIR.FAB.

Art. 151. O Órgão Central do STI elaborará e manterá atualizadas as regulamentações específicas, estabelecendo os processos de atendimento aos incidentes de segurança da informação e de prática forense computacional, em auxílio à coleta de evidências no âmbito do STI.

Art. 152. O Órgão Central do STI produzirá e divulgará conhecimentos baseados na análise dos relatórios estatísticos referentes aos atendimentos a incidentes de segurança da informação, objetivando eliminar a falha de segurança explorada ou minimizar a ocorrência dessas situações.

CAPÍTULO IX
DISPOSIÇÕES FINAIS

Art. 153. Os casos não previstos serão submetidos à apreciação do Diretor de Tecnologia da Informação da Aeronáutica.

ANEXO II

TERMO DE RESPONSABILIDADE E DE CONHECIMENTO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO COMAER (POSIN) E DAS POLÍTICAS DE SEGURANÇA DA INFORMAÇÃO DEFINIDAS PELAS RESPECTIVAS ORGANIZAÇÕES

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
DIRETORIA DE TECNOLOGIA DA INFORMAÇAO DA AERONAUTICA

Declaro que tenho pleno conhecimento de minha responsabilidade quanto à proteção a ser mantida sobre os assuntos sigilosos a que, por força de função ou atividade, tenha ou venha a ter acesso, comprometendo-me a guardar o sigilo necessário, de acordo com o que preceitua a Lei n°7.170, de 14 de dezembro de 1983, que em seu Art. 13 prevê:

"Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.

Pena: reclusão de 3 a 15 anos.
Parágrafo único - incorre na mesma pena quem:

I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;

III - oculta ou presta auxílio a espião sabendo-o tal, para subtraí-lo à ação de autoridade pública;

IV - obtém ou revela, para fim de espionagem desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em

V - desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo."

Comprometo-me em manter o sigilo de todas as minhas senhas de acesso, as quais não deverão ser fornecidas a qualquer outra pessoa.

Comprometo-me a não permitir o acesso ao meu equipamento por qualquer outra pessoa, salvo em estrita necessidade do serviço, devidamente autorizado e sob minha total

responsabilidade.

Comprometo-me a tratar de forma adequada todas as informações, documentos, softwares e instalações de caráter sigiloso com as quais venha a ter contato, não divulgando a terceiros conhecimentos restritos de qualquer natureza.

Comprometo-me a informar imediatamente à administração toda e qualquer quebra de sigilo ou de segurança, que venha a ter ciência, de forma voluntária ou não.

Comprometo-me a cumprir rigorosamente as normas de segurança em vigor no âmbito da DTI.

Estou ciente de que minha estação de trabalho poderá ser auditada pelos órgãos responsáveis, a qualquer tempo e sem aviso prévio, sendo que a nenhum diretório poderá ser negado o acesso.

Sei também que os computadores do COMAER, os seus sistemas de informação e as suas redes estão sujeitos ao monitoramento, a qualquer tempo, e que o uso dos seus recursos implica no consentimento para este monitoramento. Consequentemente, nenhuma expectativa de privacidade deve ser assumida com relação às informações transmitidas, recebidas ou armazenadas nas redes que integram a INTRAER.

Declaro ainda que estou ciente das determinações contidas nas seguintes legislações e suas atualizações, bem como das demais normas castrenses vigentes:

Termos de Uso das Mídias Sociais do COMAER, 2ª Edição. DCA 14-7/2013 - Política do COMAER para a TI;

DCA 14-8/2013 - Política de segurança da informação do COMAER;
ICA 7-5/2001 - Uso da Rede Mundial de Computadores - INTERNET - no COMAER; ICA 200-12/2013 - Avaliação de documentos classificados no COMAER;

NSCA 7-1/2012 - Uso da Rede de Dados do COMAER - INTRAER; NSCA 7-13/2013 - Segurança de Sistemas de TI no COMAER;

FCA 200-6/2013 - Tratamento de informações classificadas no COMAER; RICA 21-236/2011 - Regimento Interno da DTI

Lei 9.609, de 19 de fevereiro de 1998 - Lei da propriedade intelectual de programa de computador;

Lei 12.527, de 18 de novembro de 2011 - Lei de acesso à informação (LAI); Decreto 7.724, de 16 de maio de 2012 - Regulamenta a LAI.

Decreto 7.845, de 14 de novembro de 2012 - Regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada.

O descumprimento das mesmas ou de qualquer norma de segurança, poderá implicar nas sanções administrativas e legais julgadas cabíveis.

(Local), (dia) de (mês) de (ano).

Nome completo: _____

Assinatura: _____

Identidade/Órgão Expedidor: _____

ANEXO III
TERMO DE RESPONSABILIDADE PARA USO DE INTERNET E MÍDIAS SOCIAIS

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

Nome Completo:	
Posto/Grad:	**OM:**
CPF:	**E-mail:**

Acessos solicitados	**Justificativa:**
☐ **COM** acesso às mídias sociais	☐ **SEM** acesso às mídias sociais
☐ Acesso **PROVISÓRIO**	☐ Acesso **DEFINITIVO**
Preencha com o tipo de solicitação ((I) Inclusão; (A) Alteração; (E) Exclusão): ☐	

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 do acesso ao 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.

1. Finalidade

1.1. Este Termo de Responsabilidade estabelece os direitos, responsabilidades e obrigações relacionadas ao tratamento de dados pessoais e ao uso adequado da rede Intraer no COMAER. Ao utilizar a rede Intraer, você está concordando com os termos e condições estabelecidos neste normativo.

2. Responsabilidades

Cláusula 1 - Reconheço que é proibido o uso da rede Intraer para fins não autorizados, incluindo, mas não se limitando a: acesso a informações confidenciais sem autorização, disseminação de conteúdo ilegal ou prejudicial, violação de direitos autorais, envio de spam ou realização de atividades fraudulentas.

Cláusula 2 - Reconheço que sou responsável por manter minhas credenciais de acesso à rede Intraer em sigilo e não as compartilhar. Qualquer atividade realizada por meio de minhas credenciais será de minha inteira responsabilidade.

Cláusula 3 – Estou ciente de que as senhas de acesso têm caráter sigiloso, **sendo minha responsabilidade zelar pelo seu sigilo**, evitando:

a) Revelar a senha a quem quer que seja ou sob qualquer justificativa;

b) Anotá-la ou registrá-la em qualquer meio visível por terceiros.

Cláusula 4 - **Declaro estar ciente** de que o órgão competente pode monitorar a utilização da rede Intraer para fins de segurança, conformidade com as políticas estabelecidas e investigações internas, passível de penalidades previstas na legislação em vigor.

Cláusula 5 - Comprometo-me ser responsável pelos acessos a mim confiados, como também observar as cláusulas presentes neste instrumento.

Cláusula 6 - Comprometo-me a respeitar o grau de sigilo atribuído às informações a mim confiadas ou que venha a ter conhecimento em função da execução de atividades por mim desenvolvidas, para atendimento dos objetivos do COMAER.

Cláusula 7 - Estou ciente que a utilização da Internet deve ser exclusivamente para apoiar as atividades de
interesse doCOMAER, sendo vedada a sua utilização que, direta ou indiretamente, não esteja voltada para o atendimento dos objetivos do COMAER.

Cláusula 8– Estou ciente de que o *login* e senha são únicos e intransferíveis, sendo vedado compartilhamento. Também estou ciente que o acesso é monitorado e passível de penalidades previstas na legislação em vigor.

Cláusula 9 – Comprometo-me a colaborar, no que couber, para que a Subdivisão de Suporte do CCA-BR mantenha o Sistema Operacional e o *software* antivírus corporativo, padronizado pelo Órgão Central do STI, atualizados no computador onde está sendo utilizado o acesso, sob pena de ter o acesso revogado, caso seja detectada alguma ação maliciosa proveniente de atividade de *malware*.

Cláusula 10 – Estou ciente de que as senhas de acesso têm caráter sigiloso, **sendo minha responsabilidade zelar pelo seu sigilo**, evitando:

a) Revelar a senha a quem quer que seja ou sob qualquer justificativa; e

b) Anotá-la ou registrá-la em qualquer meio visível por terceiros.

Cláusula 11 – Declaro que devo informar imediatamente ao CTIR.FAB caso seja detectado algum evento relacionado ao acesso à Internet que possa comprometer a segurança da Informação.

Cláusula 12 – Declaro que tenho o conhecimento de que todas as minhas ações nos sistemas

do COMAER podem ser registradas e posteriormente averiguadas pelo órgão competente, **sem prejuízo das ações disciplinares e/ou criminais** que possam ser tomadas.

Cláusula 13 – Comprometo-me responder por possíveis fugas de dados e aumento de vulnerabilidades causados por ações inerentes ao acesso disponibilizado.

Cláusula 14 – Comprometo-me responder por ações cibernéticas maliciosas por uso indevido do acesso disponibilizado.

Cláusula 15 – Declaro, finalmente, estar ciente da obrigação de preservar os recursos tecnológicos a mim confiados e que o descumprimento dos itens constantes neste instrumento e das normas de segurança do COMAER serão tratados como atos de transgressão disciplinar, podendo acarretar ainda, no que couber, processos administrativos e judiciais na esfera criminal.

TABELA DE TEMPORALIDADE (TT)

Título	Descrição	Corrente	Destinação
Dados pessoais	Compreende os dados necessários para a inclusão deacesso ao **Proxy corporativo**	Prazo de vigência (1 ano)	Eliminação

(Local), (dia) de (mês) de (ano).

_____
Assinatura do solicitante

_____
Assinatura do
Comandante/Chefe/Diretor OM

ANEXO IV
TERMO DE RESPONSABILIDADE PARA USUÁRIOS DA REDE INTRAER

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

Nome Completo:	
Posto/Graduação:	**OM:**
CPF:	**E-mail:**

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 do acesso ao 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.

1. Finalidade

1.1. Este Termo de Responsabilidade estabelece os direitos, responsabilidades e obrigações relacionadas ao tratamento de dados pessoais e ao uso adequado da rede Intraer no COMAER. Ao utilizar a rede Intraer, você está concordando com os termos e condições estabelecidos neste normativo.

2. Responsabilidades

Cláusula 1 - Reconheço que é proibido o uso da rede Intraer para fins não autorizados, incluindo, mas não se limitando a: acesso a informações confidenciais sem autorização, disseminação de conteúdo ilegal ou prejudicial, violação de direitos autorais, envio de spam ou realização de atividades fraudulentas.

Cláusula 2 - Reconheço que sou responsável por manter minhas credenciais de acesso à rede Intraer em sigilo e não as compartilhar. Qualquer atividade realizada por meio de minhas credenciais será de minha inteira responsabilidade.

Cláusula 3 – Estou ciente de que as senhas de acesso têm caráter sigiloso, **sendo minha responsabilidade zelar pelo seu sigilo**, evitando:

a) Revelar a senha a quem quer que seja ou sob qualquer justificativa;

b) Anotá-la ou registrá-la em qualquer meio visível por terceiros.

Cláusula 4 - **Declaro estar ciente** de que o órgão competente pode monitorar a utilização da rede Intraer para fins de segurança, conformidade com as políticas estabelecidas e investigações internas, passível de penalidades previstas na legislação em vigor.

Cláusula 5 – Declaro que tenho o conhecimento de que todas as minhas ações na rede Intraer do COMAER podem ser registradas e posteriormente averiguadas pelo órgão competente, **sem prejuízo das ações disciplinares e/ou criminais** que possam ser tomadas.

Cláusula 6 - Reconheço que o uso indevido da rede Intraer, em violação às políticas e diretrizes estabelecidas, poderá resultar em medidas disciplinares, conforme os regulamentos internos do COMAER.

Cláusula 7 - Comprometo-me a respeitar o grau de sigilo atribuído às informações a mim confiadas ou que venha a terconhecimento em função da execução de atividades por mim desenvolvidas, para atendimento dos objetivos do COMAER.

Cláusula 8 - Estou ciente que a utilização da Intraer deve ser exclusivamente para apoiar as atividades de interesse do COMAER, sendo vedada a sua utilização que, direta ou indiretamente, não esteja voltada para o atendimento dos objetivos do COMAER.

Cláusula 9 - Comprometo-me a não divulgar, compartilhar ou utilizar indevidamente os dados pessoais de outros usuários da rede Intraer.

Cláusula 10 - Comprometo-me a cumprir as políticas e diretrizes estabelecidas por este normativo, bem como as leis e regulamentos em vigor

Cláusula 11 - Comprometo-me ser responsável pelos acessos a mim confiados, como também observar as cláusulas presentes neste instrumento.

Cláusula 12 - **Declaro estar ciente** de todo o conteúdo da **NSCA 7-13,** de 02 maio 2022, **SEGURANÇA DAINFORMAÇÃO E DEFESA CIBERNÉTICA NAS ORGANIZAÇÕES DO COMANDO DA AERONÁUTICA,** a fim de contribuir para a confidencialidade, a integridade, a disponibilidade e a autenticidade das informações armazenadas, processadas ou em trânsito na rede Intraer do COMAER.

Cláusula 13 – Declaro, finalmente, estar ciente da obrigação de preservar os recursos tecnológicos a mim confiados e que o descumprimento dos itens constantes neste instrumento e das normas de segurança do COMAER serão tratados como atos de transgressão disciplinar, podendo acarretar ainda, no que couber, processos administrativos e judiciais na esfera criminal.

CONTINUAÇÃO DO ANEXO IV – TERMO DE RESPONSABILIDADE PARA USUÁRIOS DA REDE INTRAER

TABELA DE TEMPORALIDADE (TT)

Título	Descrição	Corrente	Destinação
Dados pessoais	Compreende os dados necessários para a inclusão de acesso à **rede INTRAER do COMAER**	Prazo de vigência (1 ano)	Eliminação

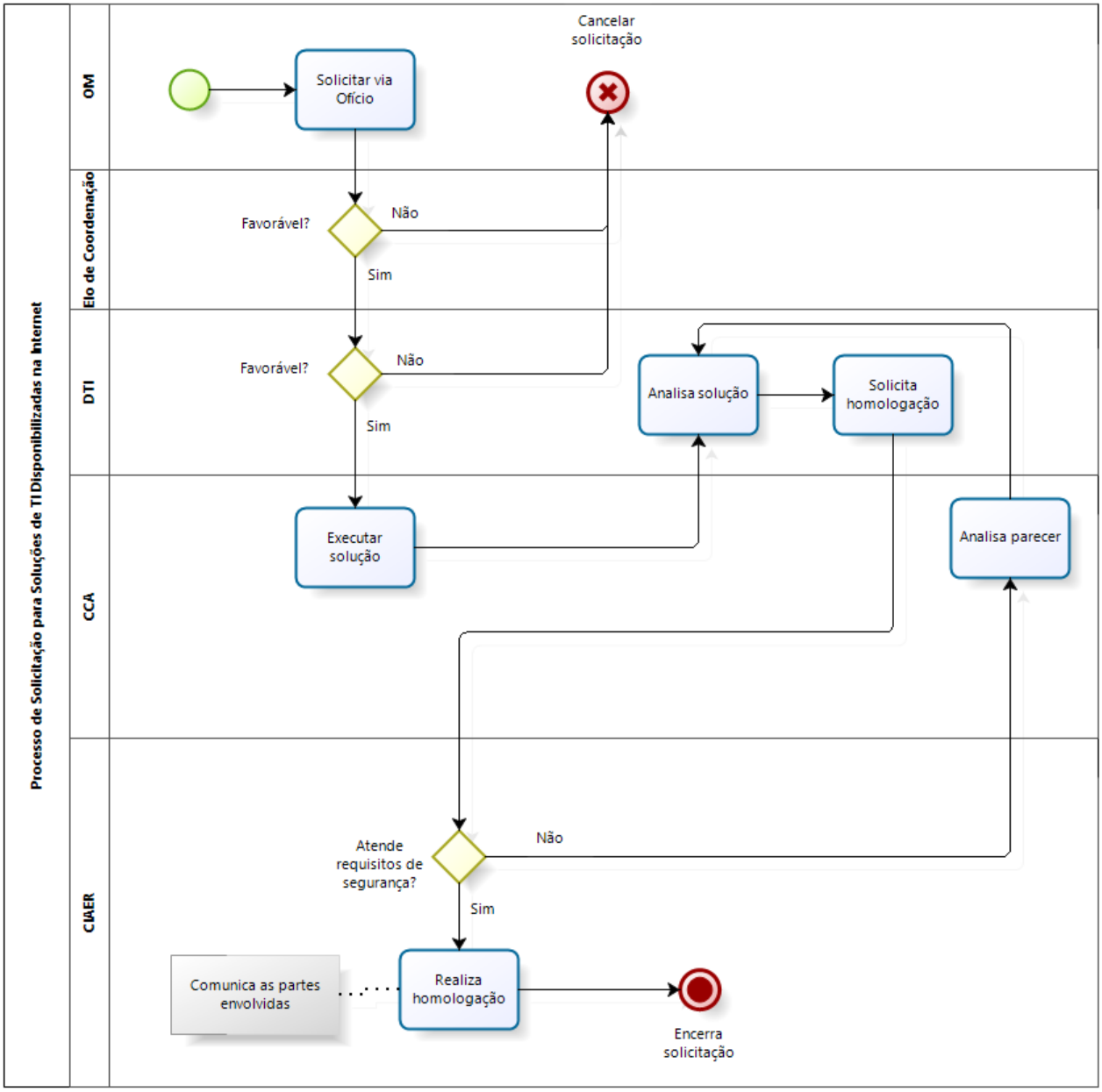
(Local), (dia) de (mês) de (ano).

_____
Assinatura do solicitante

_____
Assinatura do
Comandante/Chefe/Diretor OM

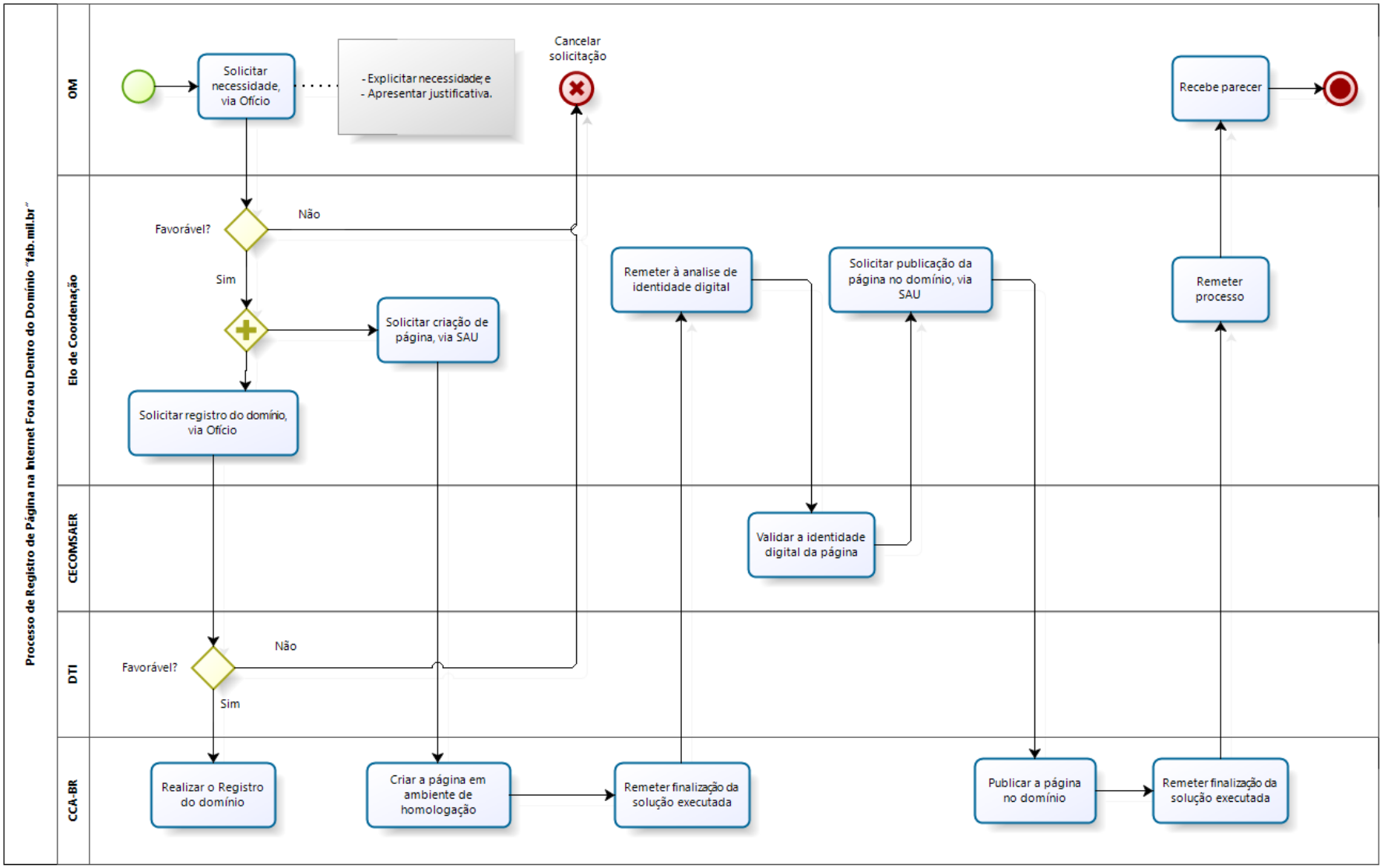
ANEXO V

PROCESSO DE SOLICITAÇÃO PARA SOLUÇÕES DE TI DISPONIBILIZADAS NA INTERNET



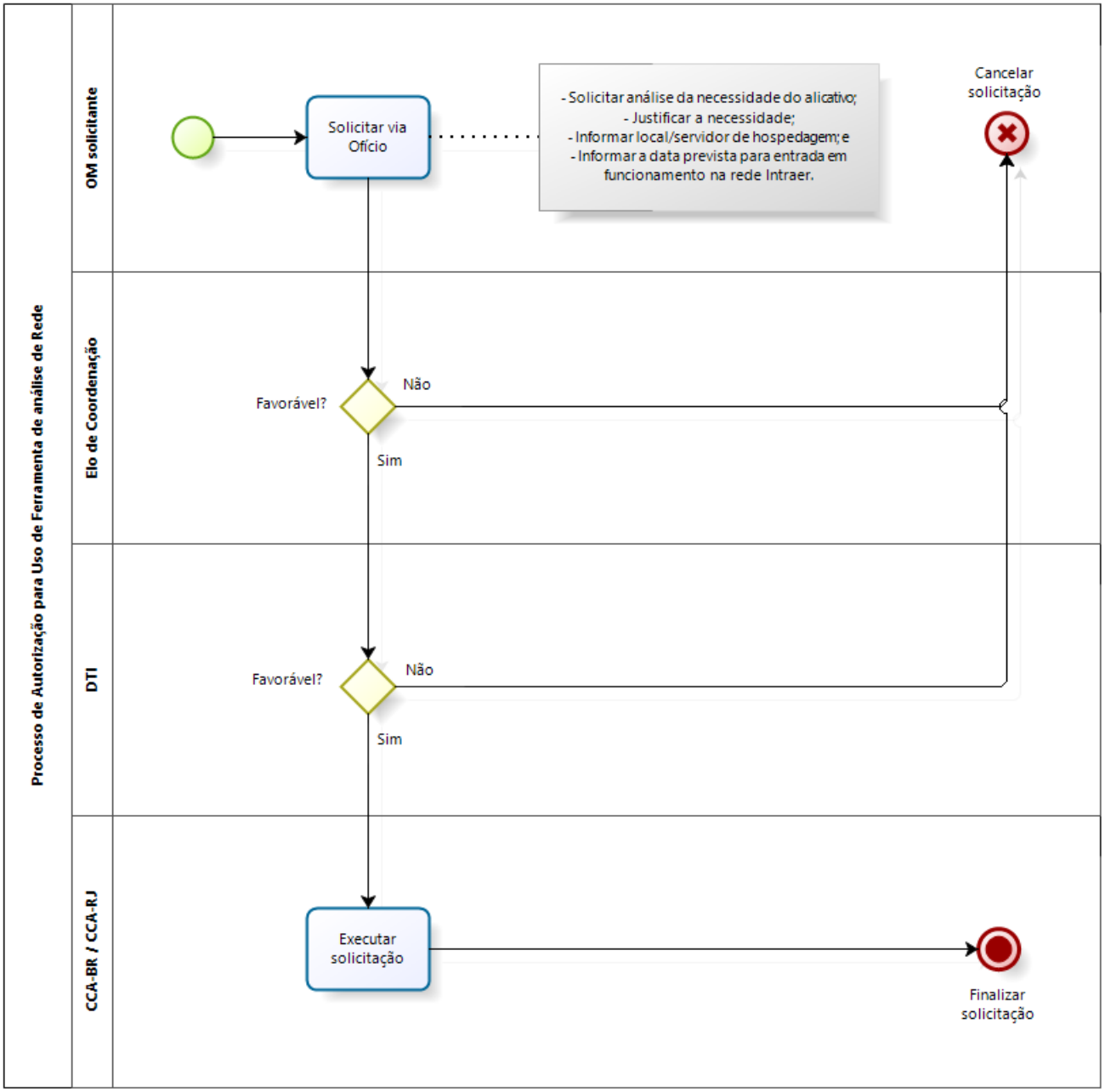
ANEXO VI

PROCESSO DE RESGISTRO DE PÁGINA NA INTERNET FORA OU DENTRO DO DOMÍNIO "FAB.MIL.BR"

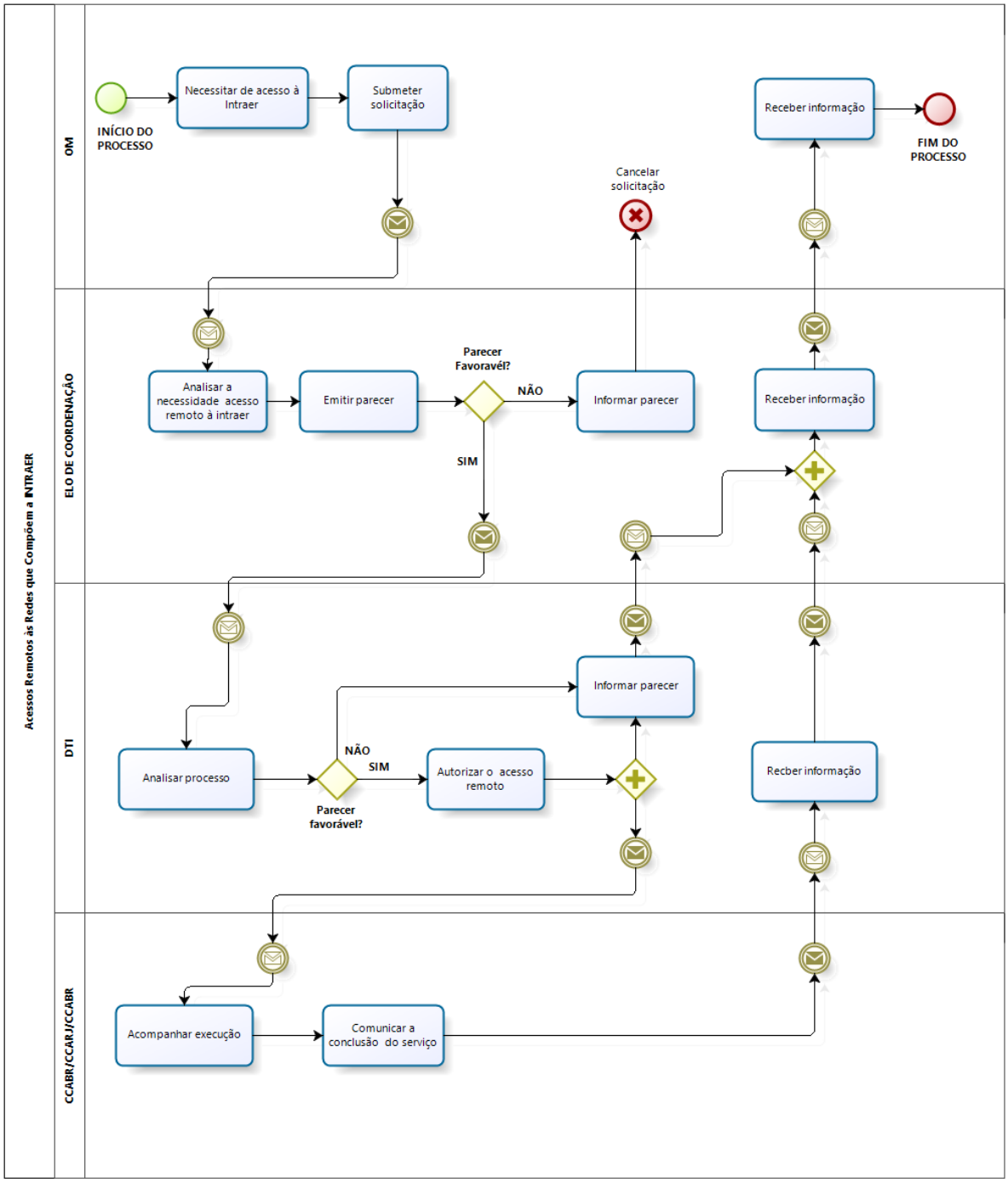


ANEXO VII

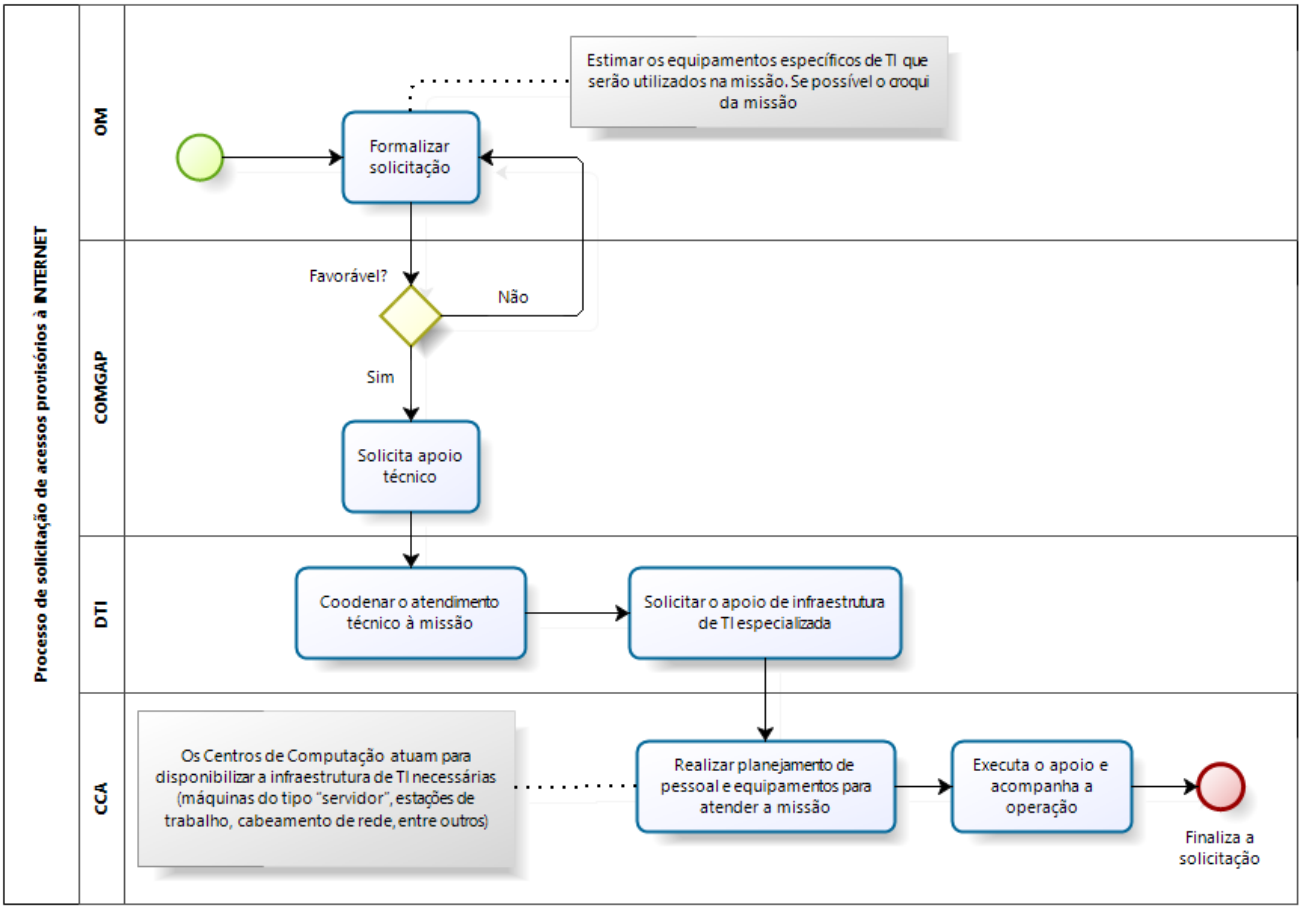
PROCESSO DE AUTORIZAÇÃO PARA USO DE FERRAMENTA DE ANÁLISE DE REDE



ANEXO VIII
PROCESSO DE ACESSO REMOTO ÀS REDES QUE COMPÕEM A INTRAER

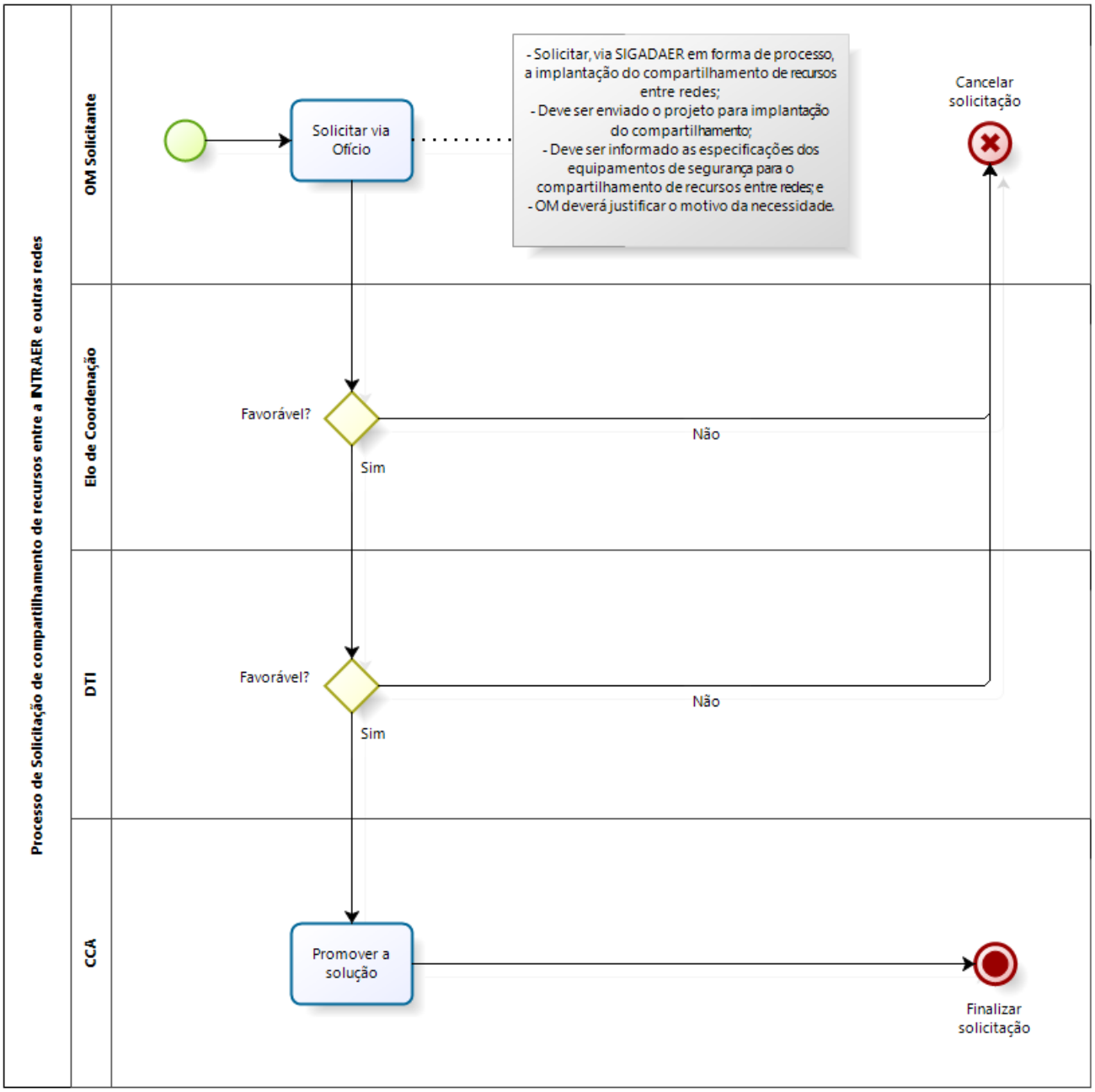


ANEXO IX
PROCESSO DE SOLICITAÇÃO DE ACESSOS PROVISÓRIOS À INTERNET



ANEXO X

PROCESSO DE SOLICITAÇÃO DE COMPARTILHAMENTO DE RECURSOS ENTRE A INTRAER E OUTRAS REDES



ANEXO XI

PROCESSO DE IMPLANTAÇÃO DE SOLUÇÕES DE TI QUE UTILIZAM RECURSOS DA INTRAER