MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA
CENTRO DE COMPUTAÇÃO DA AERONÁUTICA DO RIO DE JANEIRO

ESTRATÉGIA DE USO DE SOFTWARE E COMPUTAÇÃO EM NUVEM

Dispõe sobre a estratégia de uso de software e computação em nuvem para o Centro de Computação da Aeronáutica do Rio de Janeiro (CCA-RJ).

CAPÍTULO I
DO ESCOPO

Art. 1° A estratégia de uso de *software* e computação em nuvem tem o objetivo de assegurar que o CCA-RJ obtenha os resultados esperados e mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito da Diretoria de Tecnologia da Informação (DTI).

Art. 2° Esta estratégia deve ser aplicada para novas contratações de *software* e computação em nuvem no âmbito da DTI, tais como:

I - *software* sob o modelo de licenciamento permanente de direitos de uso;

II - *software* sob o modelo de cessão temporária de direitos de uso;

III - *software* sob o modelo de subscrição ou como Serviço (SaaS);

IV - Infraestrutura como Serviço (IaaS);

V - Plataforma como Serviço (PaaS);

VI - suporte técnico para *software* e serviços de computação em nuvem;

VII - serviço de operação e gerenciamento de recursos em nuvem;

VIII - serviço de migração de recursos para ambiente de nuvem;

IX - integração de serviços de computação em nuvem; e

X - consultoria especializada em *software* e/ou serviços de computação em nuvem.

CAPÍTULO II
DAS REFERÊNCIAS

Art. 3º Para o desenvolvimento da estratégia de uso de *software e* computação em nuvem, cabe ao CCA-RJ observar, sem prejuízo das demais normas em vigor:

I - Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 que estabelece modelo de contratação de *software* e computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

II – Normas de Segurança como ABNT NBR ISSO/IEC 27001, 27017, 27018, 27701;

III – NIST SP 800-145 que define computação em nuvem; e

IV - demais leis, decretos, resoluções, portarias e instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República.

CAPÍTULO III
DOS CONCEITOS E DEFINIÇÕES

Art. 4° Para fins de compreensão dos termos utilizados nesta norma serão considerados os seguintes conceitos e definições:

a) Atualização de versões: disponibilização, por parte do fabricante, de uma versão completa do *software*, ou parcial, mas com funcionalidades adicionais ou evoluções tecnológicas que compreendam uma nova versão estável do produto. Podem, também, incluir correções de comportamentos disfuncionais que não tenham sido corrigidos por manutenções anteriores do *software*, por critério do fabricante;

b) Catálogo de Serviços de Computação em Nuvem Padronizados: relação de serviços de computação em nuvem que um órgão ou entidade fornece aos seus usuários, elaborada de forma padronizada, de acordo com as necessidades do órgão ou entidade e conforme as orientações estabelecidas pela SGD;

c) Catálogo de Soluções de TIC com condições padronizadas: relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP, podendo incluir o nome da solução, descrição, níveis de serviço, Preço Máximo de Compra de Item de TIC - PMC-TIC, entre outros;

d) Carga de trabalho (workload): conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um ou mais serviços de TIC. As cargas de trabalho podem requerer uma combinação de recursos computacionais e de serviços técnicos para agregar valor ao negócio por meio de serviços de TIC;

e) Co-location: locação de infraestrutura de data center pertencente a terceiros para hospedar equipamentos computacionais de uma organização;

f) Computação em nuvem: modelo que possibilita o provisionamento e a utilização sob demanda de recursos e serviços computacionais de qualquer lugar e a qualquer momento, de maneira conveniente, com acesso por meio de rede a recursos configuráveis (ex.: redes, segurança, servidores, armazenamento,

aplicações e serviços) que podem ser rapidamente provisionados, utilizados e liberados com o mínimo de esforço em gerenciamento ou interatividade com o provedor de serviços em nuvem;

g) Data center ou centro de dados: Consiste em uma estrutura, ou grupo de estruturas, dedicada à acomodação centralizada, interconexão e operação dos equipamentos de tecnologia da informação e redes de telecomunicações que fornece serviços de armazenamento de dados, processamento e transporte, em conjunto a todas as instalações e infraestruturas de distribuição de energia e controle ambiental, juntamente com os níveis necessários de recuperação e segurança requeridos para fornecer a disponibilidade de serviço desejada, conforme ABNT NBR ISO/IEC 22.237-1:2023;

h) Disponibilidade: condição de um serviço ou recurso estar acessível e apto para desempenhar plenamente suas funções, em determinado momento ou durante um período acordado;

i) Incidente: qualquer acontecimento não planejado que cause redução na qualidade do serviço ou interrupção do serviço em parte ou como um todo, ou evento que ainda não impactou o serviço do usuário;

j) Incidente de Segurança da Informação: qualquer evento de segurança da informação indesejável e inesperado, seja único ou em série, que pode comprometer as operações de negócio e ameaçar a segurança da informação;

k) IN GSI/PR nº 5, de 2021: Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que dispõe sobre os requisitos mínimos de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

l)IN SGD/ME nº 94, de 2022: Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal;

m) Integrador de Serviços em Nuvem (Cloud Broker): realiza a integração dos serviços de computação em nuvem com agregação de valor entre o órgão ou a entidade e dois ou mais provedores de serviço de computação em nuvem. O Cloud Broker apoia o órgão ou entidade em descobrir, planejar, migrar, configurar, utilizar, gerenciar e evoluir os serviços de computação em nuvem de forma segura e eficiente. Os serviços prestados pelo Cloud Broker são orientados de acordo com os padrões internacionais relevantes, como a ISO e a NIST e, no Brasil, a Associação Brasileira de Normas Técnicas - ABNT, para garantir que os serviços sejam oferecidos de forma segura, eficiente e confiável;

n) Licença de *software*: documento que fornece diretrizes legalmente vinculantes para o uso e a distribuição de determinado *software*. A licença de *software* geralmente fornece aos usuários finais o direito a uma ou mais cópias do *software* sem incorrer em violação de direitos autorais. Também define as responsabilidades das partes envolvidas no contrato de licença. Além disso, pode impor restrições sobre como o *software* pode ser usado. Os termos e condições de licenciamento de *software* geralmente incluem o uso justo do *software*, as limitações de responsabilidade, garantias e isenções de responsabilidade e proteções se o *software* ou seu uso infringirem os direitos de propriedade intelectual de terceiros;

o) Licença de uso: instrumento que estabelece o direito de usar o *software* sem haver a transferência da sua propriedade entre o licenciante e o licenciado, e inclui, entre outros direitos, o serviço de correção de erros, sem ônus ao licenciado;

p) **Licença por subscrição/assinatura:** permite aos usuários acessar o *software* por meio de serviços online, em vez de adquirir uma licença de uso único. As licenças por assinatura também podem fornecer aos usuários acesso a atualizações de *software*, suporte técnico e outros serviços;

q) **Modelos de implantação de nuvem:** representam como a computação em nuvem pode ser organizada, com base no controle e no compartilhamento de recursos físicos ou virtuais. Os modelos de implantação em nuvem incluem: nuvem pública, nuvem privada, nuvem comunitária e nuvem híbrida;

r) **Modelo de Serviços em nuvem IaaS (Infrastructure as a Service - Infraestrutura como Serviço):** capacidade fornecida ao cliente para provisionar processamento, armazenamento, comunicação de rede e outros recursos de computação fundamentais, nos quais o cliente pode instalar e executar *software* em geral, incluindo sistemas operacionais e aplicativos. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, mas tem controle sobre os sistemas operacionais, armazenamento e aplicativos instalados e, possivelmente, um controle limitado de alguns componentes de rede;

s) **Modelo de Serviços em nuvem PaaS (Platform as a Service – Plataforma como Serviço):** capacidade fornecida ao cliente para provisionar na infraestrutura de nuvem aplicações adquiridas ou criadas para o cliente, desenvolvidas com linguagens de programação, bibliotecas, serviços e ferramentas suportados pelo provedor de serviços em nuvem. O cliente não gerencia nem controla a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tem controle sobre as aplicações instaladas e possivelmente sobre as configurações do ambiente de hospedagem de aplicações;

t) **Modelo de Serviços em nuvem SaaS (*software* as a Service – *software* como Serviço):** capacidade de fornecer uma solução de *software* completa que pode ser contratada de um provedor de serviços em nuvem. Toda a infraestrutura subjacente, middleware, *software* de aplicativo e dados de aplicativo ficam no data center do provedor de serviços. O provedor de serviço gerencia hardware e *software* e garante a disponibilidade e a segurança do aplicativo e de seus dados;

u) **Multinuvem (multicloud**): uma estratégia de utilização dos serviços de computação em nuvem por meio de dois ou mais provedores de nuvem pública;

v) **Nuvem híbrida:** infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

w) **Nuvem privada ou interna** - infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade pode ser do próprio órgão ou de empresas públicas com finalidade específica relacionada à tecnologia da informação, conforme ISO/IEC 22123-1:2023 (Information technology — Cloud computing — Part 1: Vocabulary). O modelo de nuvem privada admite o uso de recursos computacionais de provedores de nuvem pública somente se assegurado o isolamento lógico e físico desses recursos, no ambiente do próprio órgão ou de empresas públicas, e não se configurando como uso de Nuvem Pública;

x) **Nuvem pública ou externa** - infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de órgãos públicos, empresas privadas ou de ambos;

y) **Provedor de serviços em nuvem:** empresa que possui infraestrutura de Tecnologia da Informação - TI destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem;

z) **Serviço:** meio de entregar valor aos usuários internos ou externos à organização ao facilitar o alcance de resultados almejados;

aa) ***software*** **livre: tipo** de *software* de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O *software* livre é publicado sob uma licença que permite aos usuários acessar os códigos-fonte e modificá-los para atender às suas necessidades;

bb) ***software*** **open source (ou de código aberto):** tipo de *software* de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente. O *software* open source é publicado sob uma licença que permite aos usuários acessar o código-fonte, mas impõe certas limitações quanto a sua modificação ou personalização;

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 5° Esta estratégia segue os seguintes princípios:

I - respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;
II - garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do CCA-RJ, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;
III - alinhamento estratégico da Política de Segurança da Informação com os demais planos institucionais;
IV - responsabilidade pelo cumprimento das normas pertinentes à segurança da informação vigentes; e
V - conscientização, educação e comunicação como alicerces fundamentais para o fomento da cultura em segurança da informação.

CAPÍTULO V
DAS DISPOSIÇÕES GERAIS

Art. 6° A apresentação dos relatórios de auditoria, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com órgãos ou entidades da administração pública federal.

Parágrafo único. Na hipótese de utilização de cloud broker, esse será o responsável por apresentar os relatórios de auditoria de todos os provedores de serviço de nuvem que ele representa.

CAPÍTULO VI
DAS DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE SOFTWARE E COMPUTAÇÃO EM NUVEM

Art. 7° Diretrizes deverão ser observadas pelo CCA-RJ ao adotar soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

Seção I
Da identificação das necessidades do negócio

Art. 8° O CCA-RJ deve identificar e avaliar as necessidades de negócio antes da contratação de *software e* computação em nuvem.

Parágrafo único. Deve-se determinar quais sistemas, aplicações, dados e serviços precisam ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários.

Seção II
Da seleção dos modelos adequados

Art. 9° O CCA-RJ deve avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida etc.) melhor se adequam aos requisitos de negócio.

§1º Caso as seções do CCA-RJ não possuam maturidade suficiente na contratação de serviços em nuvem ou possua impedimentos técnicos ou normativos para migração de alguns *workloads*, é recomendável sempre dar preferência à adoção de uma abordagem estratégica de nuvem híbrida.

§2º Caso as seções do CCA-RJ possuam maturidade e já tenham concluído que a demanda prevista pode ser atendida integralmente por meio de serviços em nuvem, uma abordagem completa, incluindo as demandas de migração do ambiente *on-premises* para a nuvem pode ser adotada.

Seção III
Da avaliação dos possíveis fornecedores

Art. 10° Os estudos técnicos preliminares devem abranger o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir que exista uma quantidade mínima de fornecedores com experiência e que atendam aos requisitos necessários ao atendimento da demanda.

Parágrafo único. Fatores como segurança, conformidade, disponibilidade e suporte técnico devem ser considerados nessa avaliação.

Seção IV
Da definição de requisitos de segurança

Art. 11° O CCA-RJ deve determinar quais requisitos de segurança são importantes ou mandatórios para o negócio e deve ser avaliado, quando for o caso, como cada possível fabricante ou fornecedor atende a esses requisitos.

Seção V
Do estabelecimento de uma política de governança

Art. 12° A política de governança deve abranger a identificação e classificação de dados, controle de acesso, gerenciamento de configuração e, quando for o caso, monitoramento das atividades em nuvem, de modo a garantir que os serviços a serem contratados sejam executados em conformidade com os padrões adotados pelo CCA-RJ.

Seção VI
Das diretrizes de uso seguro de *software e* computação em nuvem

Art. 13° A DTI deve definir políticas e normas que versam sobre segurança da informação e sobre o tratamento de informações em nuvem, bem como identificar, sob essa perspectiva, quais os sistemas ou *workloads* que podem ser migrados, assim como as medidas de gerenciamento de risco a serem adotadas para resguardar as informações sigilosas que eventualmente serão tratadas em ambiente de nuvem.

Seção VII
Da avaliação quanto às condições mínimas de infraestrutura de Tecnologia de Informação do CCA-RJ para utilizar serviços de computação em nuvem

Art. 14° O CCA-RJ deve ter conexão estável com a Internet e com banda suficiente para gerenciar *softwares* e serviços de computação em nuvem.

Seção VIII
Da definição de diretrizes de governança para o uso da nuvem

Art. 15° O CCA-RJ deve definir papéis e responsabilidades para as áreas de TI, de negócio e da nuvem.

Seção IX
Do estabelecimento dos princípios norteadores da estratégia

Art. 16° O CCA-RJ deve adotar os seguintes princípios norteadores da estratégia:

I - *adoção preferencial de estratégias Cloud Smart e Hybrid-by-Design;*

II - *priorização de arquiteturas resilientes, interoperáveis e escaláveis;*

III - *utilização racional de ambientes multicloud, observando governança centralizada, otimização de custos e mitigação de dependência tecnológica;*

IV - *priorização de modernização arquitetural em detrimento de simples migração de cargas legadas; e*

V - *adoção de princípios de segurança Zero Trust e automação de infraestrutura*.

Seção X
Do alinhamento com outros planos estratégicos

Art. 17° Esta estratégia deve estar alinhada com os planos estratégicos da DTI e do Comando da Aeronáutica.

Seção XI
Do estabelecimento de linhas de base e metas de benefícios/resultados esperados

Art. 18° O CCA-RJ deve definir linhas de base e metas de benefícios/resultados esperados objetivando maior agilidade, redução de custos, resiliência e mais segurança.

Seção XII
Das considerações sobre capacitação da equipe

Art. 19° O CCA-RJ deve capacitar a equipe que gerenciará, operará ou utilizará os recursos de *software* e de computação de serviços em nuvem, identificando as capacidades e habilidades necessárias.

Seção XIII
Das considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços

Art. 20° O CCA-RJ deve considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

Seção XIV
Dos requisitos regulatórios e de conformidade

Art. 21° O CCA-RJ deve considerar os requisitos regulatórios e de conformidade para o uso seguro de *software* e serviços de computação em nuvem no âmbito da DTI e da administração pública federal.

Seção XV
Da indicação da estratégia de saída

Art. 22° O CCA-RJ deve considerar a análise de dependências e aspectos de portabilidade (*backup*, redundância, contratos de apoio, retorno para a infraestrutura local etc.)

Seção XVI
Da análise de riscos

Art. 23° O CCA-RJ deve considerar as diretrizes de gerenciamento de riscos constantes no modelo de contratação de *software e* computação em nuvem estabelecidos na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 ou documento equivalente publicado posteriormente.

CAPÍTULO VII
DA DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 24° O CCA-RJ trata os requisitos para uso seguro de computação em nuvem em norma específica para esta finalidade.

CAPÍTULO VIII
DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

Seção I
Da Alta Administração

Art. 25° Compete à alta administração:
I - assegurar a utilização de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento; e
II - disponibilizar recursos financeiros e humanos para a implementação desta estratégia.

Seção II
Do Comitê de Segurança da Informação

Art. 26° Compete ao Comitê de Segurança da Informação:

I - aprovar as minutas de elaboração e de revisões de atos normativos sobre estratégia e o uso seguro de computação em nuvem e divulgá-las às partes interessadas;
II - estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;
III - definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e
IV - analisar, em caráter conclusivo, as minutas de elaboração e de revisões de ato normativo sobre estratégia e o uso seguro de computação em nuvem.

Seção III
Do Gestor de Segurança da Informação

Art. 27° Compete ao Gestor de Segurança da Informação:

I - instituir e coordenar a equipe para elaboração e revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem;

II - supervisionar a aplicação do ato normativo sobre estratégia e o uso seguro de computação em nuvem;
III - assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, de forma a assegurar que os controles e os níveis de serviço relacionados à segurança da informação acordados sejam cumpridos;
IV - supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios relacionados à segurança da informação;
V - comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;
VI - encaminhar para aprovação da alta administração as minutas de elaboração e de revisões de ato normativo sobre o uso seguro de computação em nuvem; e
VII - propor ações de segurança da informação para a implementação ou a contratação de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento.

Seção IV
Da Divisão Técnica e demais setores de TI do CCA-RJ

Art. 28° Compete à Divisão Técnica e demais setores de TI do CCA-RJ:

I - implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem em conformidade com as orientações contidas neste documento e legislação pertinente.

CAPÍTULO IX
DA REVISÃO E ATUALIZAÇÃO

Art. 29° Esta estratégia e os documentos gerados a partir dela devem ser revisados, aprovados e atualizados em função de alterações na legislação pertinente, de diretrizes políticas do governo federal, de alterações nas políticas e normas da DTI, quando considerada necessária pelo Comitê de Segurança da Informação.

Art. 30° Em função da capacidade de os provedores de serviço de computação em nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a presente estratégia deve ser revisada em até 2 (dois) anos para:

I - definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;
II - atualizar periodicamente os processos internos de gestão de riscos de segurança da informação;
III - quando ocorrerem eventos, fatores relevantes, novos requisitos tecnológicos, corporativos e/ ou legais que exijam sua revisão imediata; e
IV - assegurar a continuidade, sustentabilidade, adequação e efetividade quando houver mudanças significativas nos requisitos de segurança da informação que influenciam o uso seguro da computação em nuvem.

CAPÍTULO X
DAS DISPOSIÇÕES FINAIS

Art. 31° As novas contratações de *software* e computação em nuvem devem observar as diretrizes apresentadas neste documento, bem como o modelo de contratação de *software e* computação em nuvem, no âmbito dos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.

Art. 32° Esta estratégia e seus documentos complementares devem ser divulgados a todos os usuários e partes interessadas a fim de promover sua observância e conhecimento.

Art. 33° A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

Art. 34° Os casos omissos não abordados neste documento serão analisados pelo Comitê de Segurança da Informação da DTI.

Rio de Janeiro, 01 de junho de 2026.

TCEL QOENG CMP EDNELSON SILVA DE **OLIVEIRA**
Chefe da Divisão Técnica (DT) do CCA-RJ

CEL QOINT RODRIGO MORO **LOUREIRO**
Chefe do CCA-RJ

MINISTÉRIO DA DEFESA
COMANDO DA AERONÁUTICA

CONTROLE DE ASSINATURAS ELETRÔNICAS DO DOCUMENTO

Documento:	ESTRATÉGIA DO USO DE SOFTWARE E COMPUTAÇÃO EM NUVEM
Data/Hora de Criação:	01/06/2026 18:48:16
Páginas do Documento:	11
Páginas Totais (Doc. + Ass.)	12
Hash MD5:	2554a027453d32f7f1f80f5d808a0eed
Verificação de Autenticidade:	https://autenticidade-documento.sti.fab.mil.br/assinatura

Este documento foi assinado e conferido eletronicamente com fundamento no artigo 6º, do Decreto nº 8.539 de 08/10/2015 da Presidência da República pelos assinantes abaixo:

Assinado via ASSINATURA CADASTRAL por Ten Cel Eng EDNELSON SILVA DE OLIVEIRA no dia 01/06/2026 às 16:05:05 no horário oficial de Brasília.

Assinado via ASSINATURA CADASTRAL por Cel RODRIGO MORO LOUREIRO no dia 01/06/2026 às 16:07:05 no horário oficial de Brasília.