2ª PARTE
ASSUNTOS GERAIS DA ADMINISTRAÇÃO

DO COMITÊ DE GOVERNANÇA

RESOLUÇÃO CG/PF Nº 10, DE 24 DE FEVEREIRO DE 2025

Aprova o Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal.

O COMITÊ DE GOVERNANÇA DA POLÍCIA FEDERAL, no uso das atribuições que lhe conferem o art. 8º, *caput*, incisos II e III, e § 3º, da Portaria DG/PF nº 18.703, de 27 de outubro de 2023, publicada no Boletim de Serviço nº 208, de 1º de novembro de 2023; e tendo em vista o disposto no art. 16 do Decreto nº 9.203, de 22 de novembro de 2017; e na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023; resolve:

Art. 1º Esta Resolução aprova o Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal, na forma do Anexo I.

Art. 2º Esta Resolução entra em vigor na data de sua publicação no Boletim de Serviço.

ANEXO I
DOCUMENTO DE ESTRATÉGIA DE USO DE *SOFTWARE* E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM DA POLÍCIA FEDERAL

CAPÍTULO I
DAS DISPOSIÇÕES GERAIS

Art. 1º Este Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem da Polícia Federal visa consolidar diretrizes, processos e controles essenciais para o uso racional, eficiente e seguro de soluções em nuvem no âmbito da Polícia Federal, de forma a:

I - orientar o uso de *software* e de serviços de computação em nuvem no âmbito da Polícia Federal; e

II - observar os direcionadores de utilização de *software* e de serviços de computação em nuvem, inclusive quanto aos aspectos de segurança da informação e privacidade.

Art. 2º O uso de *software* e de serviços de computação em nuvem na Polícia Federal deve primar pelo compromisso com a modernização e eficiência dos seus processos por meio da adoção estratégica de tecnologias inovadoras.

Art. 3º Este Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal reforça o compromisso da Polícia Federal em utilizar, de forma responsável, a tecnologia de computação em nuvem para tratamento de seus dados e suas soluções tecnológicas, detalhar a governança, as responsabilidades na operação dos ambientes de nuvem da Polícia Federal, bem como os requisitos de operação e segurança, e a política de tratamento de dados e cargas de trabalho que tratem informação estratégica ou com restrição de acesso prevista em legislação específica.

Art. 4º Esta estratégia deve ser aplicada para novas contratações e projetos de *software* e de serviços de computação em nuvem, 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* serviços de computação em nuvem.

CAPÍTULO II
DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para fins de compreensão dos termos utilizados nesta norma, serão considerados os seguintes conceitos e definições:

I - carga de trabalho (*workload*): conjunto de recursos que compõem uma arquitetura técnica destinada a suportar um ou mais serviços de Tecnologia da Informação e Comunicação – 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;

II - 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;

III - data center ou estrutura *on-premise*: 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;

IV - 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;

V - 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;

VI - 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;

VII - licença por subscrição/assinatura: permite aos usuários acessarem 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;

VIII - licença perpétua: é uma licença que concede ao usuário o direito de usar o *software* por tempo indeterminado, bem como acesso a updates e suporte técnico por tempo determinado;

IX - 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 de governo, nuvem comunitária e nuvem híbrida;

X - 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;

XI - 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;

XI - 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, não gerenciando nem controlando a infraestrutura na nuvem subjacente, incluindo rede, servidores, sistema operacional ou armazenamento, mas tendo controle sobre as aplicações instaladas e, possivelmente, sobre as configurações do ambiente de hospedagem de aplicações.

XII - 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;

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

XIV - nuvem comunitária: modelo de implantação de nuvem em que os serviços de computação em nuvem são exclusivamente suportados e compartilhados por um grupo específico de órgãos e entidades de serviços de computação em nuvem que têm requisitos compartilhados e um relacionamento entre si, e onde os recursos são controlados por pelo menos um membro deste grupo, conforme ISO/IEC 22123-1:2023 (*Information technology – Cloud computing – Part 1: Vocabulary*). O modelo de nuvem comunitária 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;

XV - nuvem de governo: infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas;

XVI - 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;

XVII - 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 cuja 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 e que 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;

XVIII - 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;

XIX - orquestração: habilidade de coordenar e gerenciar recursos em diferentes provedores de nuvem públicas;

XX - plataforma de gerenciamento de serviços em nuvem (*Cloud Management Platform – CMP*): sistema capaz de realizar o provisionamento e orquestração, requisição de serviço, inventário e classificação, monitoramento e análise, gerenciamento de custos e otimização de carga de trabalho, migração em nuvem, cópias de segurança e recuperação de desastres, gerenciamento de segurança, conformidade, identidade e implantação dos recursos nos provedores de nuvem ofertados;

XXI - provedor de serviços em nuvem: empresa que possui infraestrutura de TIC destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem;

XXII - serviço: meio de entregar valor aos usuários internos ou externos à organização ao facilitar o alcance de resultados almejados;

XXIII - serviços agregados: são serviços adicionais providos pelo fornecedor da solução que oferecem aos usuários acesso a recursos adicionais relacionados ao objeto principal. Esses serviços podem incluir suporte técnico, treinamento, atualizações, implementação e outros serviços;

XXIV - suporte técnico: serviço provido pelo fornecedor para auxiliar os usuários com problemas relacionados ao serviço contratado e que pode incluir resolução de problemas, treinamento, atualizações, implementação e instalação; e

XXV - tratamento da informação: conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

CAPÍTULO III
DOS OBJETIVOS, COMPETÊNCIAS E IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

Seção I
Dos objetivos e das necessidades de negócio

Art. 6º Os principais objetivos e necessidades de negócio a serem alcançados com o uso de *software* e de serviços de computação em nuvem são:

I - alcançar maior controle e administração sobre os custos com armazenamento e processamento de dados e soluções da Polícia Federal em nuvem;

II - aumentar a agilidade e a escalabilidade para armazenar e processar dados de interesse da organização;

III - melhorar a performance e a disponibilidade dos ambientes transacionais e analíticos, bem como reduzir os tempos para provimento de soluções corporativas de TIC;

IV - reduzir o intervalo de tempo entre a disponibilização de novidades tecnológicas pelo mercado e a sua efetiva utilização interna;

V - proporcionar flexibilidade no desenvolvimento e na sustentação de soluções que suportem processos de trabalho, os quais venham a ser modificados em virtude de reformas legislativas e normativos internos; e

VI - proporcionar o desenvolvimento e a sustentação de soluções disruptivas que permitam o aumento da produtividade em processos de trabalho internos e ofertas de serviço aos cidadãos.

Seção II
Dos princípios

Art. 7º Os princípios da estratégia de uso de *software* e de serviços de computação em nuvem são:

I - iniciativas de provimento de soluções tecnológicas e de modernização das soluções atualmente implementadas na Polícia Federal deverão ser avaliadas quanto à viabilidade e conveniência do uso de computação em nuvem;

II - estratégia m*ulticloud*: deverá ser adotada preferencialmente uma estratégia de *multicloud*, distribuindo cargas de trabalho entre diferentes provedores de nuvem público, de governo ou privado, aproveitando o melhor que cada provedor tem a oferecer, reduzindo risco de dependência e considerando o custo de transferência de dados entre provedores de nuvem;

III - priorização da segurança: deverão ser incorporadas medidas de segurança robustas em todas as camadas, desde o acesso e autenticação até a criptografia de dados e o monitoramento contínuo, a depender do caso prático e da viabilidade, de modo a mitigar os riscos cibernéticos e proteger os ativos mais valiosos, especialmente os dados, contra ameaças internas e externas;

IV - capacitação contínua: investimento contínuo em capacitação e desenvolvimento de competências técnicas. A Polícia Federal deve promover uma cultura de inovação e colaboração, incentivando a experimentação e o aprendizado contínuo das tecnologias de comutação em nuvem; e

V - aumentar a maturidade e a transparência na gestão dos custos relacionados ao uso dos serviços de computação em nuvem por meio de métricas estabelecidas de forma conjunta entre as áreas técnicas, negociais e de orçamento da Polícia Federal.

Seção III
Do alinhamento estratégico

Art. 8º Os projetos e ações relacionados ao uso de *softwares* e computação em nuvem na Polícia Federal deverão estar alinhados ao plano estratégico da Polícia Federal, bem como ao Plano Diretor de Tecnologia da Informação e de Comunicação – PDTIC/PF e demais instrumentos de governança e gestão de riscos.

Art. 9º Novas soluções a serem contratadas junto a fornecedores e provedores de *softwares* e serviços de computação em nuvem deverão constar no Plano de Contratações Anual – PCA ou ferramenta de governança que o substitua.

Art. 10. O uso de *softwares* e serviços de computação em nuvem deve buscar, além dos objetivos já presentes neste Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal, uma maior agilidade na adoção de novas tecnologias, com otimização e transparência dos custos e maior controle sobre aspectos relacionados à operação e segurança da informação.

Art. 11. As iniciativas que usam ou dependem da tecnologia em nuvem para a consecução de seus objetivos, a exemplo de solução que modifique processos de trabalho, deverão ser precedidas de documento que estabeleça os benefícios e resultados esperados com a adoção da solução, levando em consideração linha de base estabelecida, respeitando os normativos e artefatos específicos estabelecidos na Polícia Federal.

Seção IV
Das competências, atribuições e responsabilidades

Art. 12. Compete ao Comitê de Governança da Polícia Federal – CG/PF, no papel de Comitê de Governança Digital:

I - definir a estratégia de nuvem para a Polícia Federal; e

II - deliberar acerca da conveniência e oportunidade da priorização dos recursos financeiros e humanos a serem aplicados para a implementação da estratégia de *software* e de serviços de computação em nuvem.

Art. 13. Compete à Comissão de Dados e Tecnologia da Informação e Comunicação – CDTIC/CG/PF, acerca dos temas relacionados ao uso de recursos de nuvem e cibersegurança da Polícia Federal:

I - propor as minutas de elaboração e de revisões do ato normativo sobre estratégia e o uso seguro de computação em nuvem e divulgá-las às partes interessadas;

II - propor os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem;

III - analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo complementar acerca da estratégia e o uso seguro de computação em nuvem; e

IV - analisar, em caráter conclusivo, o envio e armazenamento de dados em nuvem.

Art. 14. 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 internos e externos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida;

VI - propor para a CDTIC/CG/PF as minutas de elaboração e de revisões do 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 de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal.

Art. 15. Compete à Diretoria de Tecnologia da Informação e Comunicação – DTI/PF:

I - assegurar a utilização de tecnologias de *software* e computação em nuvem em conformidade com as orientações contidas neste Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal;

II - implementar os procedimentos relativos ao uso de tecnologias de computação em nuvem em conformidade com as orientações contidas neste Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal e legislação pertinente; e

III - prover e gerir os componentes de *software* e de serviços de computação em nuvem conforme os princípios e diretrizes de governança estabelecidos pelo CG/PF, identificando e avaliando as necessidades de negócio antes da sua contratação, determinando quais sistemas, aplicações, dados e serviços podem ser movidos para a nuvem, como eles serão acessados e quais recursos computacionais e de armazenamento serão necessários.

CAPÍTULO IV
DAS DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE *SOFTWARE* E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

Seção I
Da seleção dos modelos adequados

Art. 16. Os modelos de uso de *softwares* e serviços de computação em nuvem (como IaaS, PaaS, SaaS), bem como suas implementações (como nuvem privada, nuvem de governo e nuvem pública), serão avaliados pela DTI/PF para que seja adotada a modalidade que melhor se adequar aos requisitos de negócio, de segurança da informação e das arquiteturas tecnológicas aprovadas para uso na instituição.

Art. 17. As cargas de trabalho que tratem informação com restrição de acesso prevista na legislação, a exemplo de: sigilo fiscal, bancário, comercial, empresarial, contábil, de segredo industrial, de direito autoral, de propriedade intelectual, industrial, policial, processual civil, processual penal e disciplinar administrativa serão mantidas, preferencialmente, em ambiente de nuvem privada.

Art. 18. Caso o modelo de nuvem privada não atenda ao que se busca com as suas respectivas entregas, poderão ser usadas nuvens de governo ou públicas, bem como suas soluções e serviços.

§ 1º Os projetos que tratem dados com restrição legal, conforme o *caput*, devem ser submetidos aos respectivos curadores e à CDTIC/CG/PF para aprovação.

§ 2º Nos documentos de visão e de arquitetura dos projetos de desenvolvimento de *software*, as áreas negociais e técnicas deverão abordar aspectos de viabilidade e conveniência do uso de serviços de computação em nuvem.

Art. 19. Para o caso de provas de conceito e projetos-piloto, a DTI/PF poderá autorizar, em ato conjunto com a área curadora dos dados, o desenvolvimento e a homologação de soluções no ambiente de computação em nuvem considerando a utilização de informação com restrição de acesso prevista na legislação, desde que previamente definida e restrita aos dados efetivamente necessários.

Seção II
Da avaliação dos possíveis fornecedores

Art. 20. Os estudos técnicos preliminares abrangerão o levantamento dos possíveis fornecedores aptos ao atendimento dos requisitos de negócio, de forma a garantir que exista uma quantidade mínima de concorrentes com experiência e que atendam aos requisitos necessários ao atendimento da demanda.

Art. 21. A DTI/PF será responsável pela coordenação da contratação de *softwares* e de serviços de computação em nuvem e conduzirá avaliações técnicas conforme os critérios estabelecidos nos planejamentos de contratação.

Art. 22. As avaliações de possíveis fornecedores poderão levar em consideração os critérios gerais que seguem, sem prejuízo de critérios específicos de cada solução:

I - tempo de execução de carga de trabalho;

II - consultas transacionais e analíticas por meio de comandos específicos sobre as tabelas geradas, medindo o desempenho (duração da consulta) em diversas condições;

III - avaliação da *performance* de recursos computacionais e respectivos custos, aplicando implementações próprias e de terceiros;

IV - comparações de resultados entre implementações próprias e as soluções ofertadas pelos provedores; e

V - testes de segurança com o objetivo de avaliar os riscos do tratamento e armazenamento de dados protegidos por estratégicos ou sigilosos em uma nuvem.

Parágrafo único. Fatores como compatibilidade com as arquiteturas tecnológicas existentes na instituição, conformidade, disponibilidade de profissionais especializados e suporte técnico dos fornecedores, dentre outros, também podem ser considerados nessa avaliação.

Seção V
Da definição de requisitos de segurança

Art. 23. Aplicam-se, sempre que cabíveis, as diretrizes, os princípios, os controles e as medidas definidas no Programa de Privacidade e Segurança da Informação e na Política de Cibersegurança da Polícia Federal.

Art. 24. Os recursos de *softwares* e serviços de computação em nuvem estabelecidos para os sistemas deverão ser logicamente segmentados.

Art. 25. Deverá ser implementa política de privilégio mínimo para acesso aos recursos, sistemas, *softwares* e serviços em computação em nuvem, priorizando processos e ferramentas de *just-in-time-access*.

Art. 26. As aplicações e as cargas de trabalho devem implementar, sempre que possível, controles para detectar e impedir a exfiltração de dados, aplicando criptografia, sempre que possível.

Art. 27. Cargas de trabalho e aplicações deverão executar periodicamente varreduras de vulnerabilidade (*scans*) em todos os recursos.

Art. 28. Os controles e medidas de segurança mínimos necessários serão definidos conforme a avaliação da criticidade de cada sistema.

Parágrafo único. A não implementação de um controle ou medida de segurança, quando inviável, deve ser feito tendo como base uma avaliação de risco prévia.

Seção VI
Do estabelecimento de uma política de governança

Art. 29. O uso de *software* e de serviços de computação em nuvem adotará, sempre que cabível, princípios, diretrizes, controles e medidas estabelecidos na política de governança de TIC da Polícia Federal e demais normas internas ou externas que tratem da identificação, classificação de dados, controle de acesso, gerenciamento de configuração e, quando for o caso, monitoramento das atividades, de modo a garantir que os serviços a serem implementados sejam executados em conformidade com os padrões estabelecidos pela Polícia Federal.

Seção VII
Diretrizes de uso seguro de *software* e de serviços de computação em nuvem

Art. 30. O uso de *software* e de serviços de computação em nuvem adotará, sempre que cabível, os princípios, diretrizes, controles e restrições de segurança aplicados aos *softwares* e equipamentos computacionais da rede interna da Polícia Federal, devendo passar pelos mesmos processos de homologação ou autorização, mesmo que em rito simplificado.

Art. 31. O uso de *softwares* ou serviços não nativamente disponibilizados pelos provedores de nuvem deve ser preferencialmente precedido por análise de risco e estudo técnico que estabeleça as diretrizes de segurança aplicáveis.

Seção VIII
Da avaliação quanto às condições mínimas de infraestrutura de TIC
do órgão ou entidade para utilizar serviços de computação em nuvem

Art. 32. Serão identificados os sistemas ou cargas de trabalho que podem ser migrados, assim como as respectivas medidas de gerenciamento de risco a serem adotadas para resguardar as informações sigilosas que eventualmente serão tratadas em ambiente de nuvem.

Art. 33. A DTI/PF deverá especificar e prover as condições mínimas de infraestrutura do ambiente da rede interna e de prestadores de serviços, no que se aplicar, ao uso de *software* e de serviços de computação em nuvem.

Art. 34. As arquiteturas tecnológicas, controles de acesso lógico, definição de perfis e outros temas afins, estabelecidos para a rede interna da Polícia Federal também devem ser aplicados, sempre que possível, ao uso de *software* e de serviços de computação em nuvem.

Seção IX
Das diretrizes de governança para o uso da nuvem

Art. 35. O uso de *software* e de serviços de computação em nuvem deverá respeitar as seguintes diretrizes:

I - cargas de trabalho e aplicações deverão ter métricas definidas para avaliar a confiabilidade do serviço, de acordo com a criticidade da carga de trabalho, arquitetura e requisitos de resiliência a falhas, além de planos de ações para recuperação de desastres;

II - provedores de identidade devem ter alta disponibilidade;

III - mecanismos de segurança nas cargas de trabalho e aplicações, como *Web Application Firewall – WAF*, *Firewall* e contra *Distributed Denial of Service* – anti-DDoS devem ser implementados;

IV - gestão segura de certificados digitais, chaves e segredos, garantindo suas cópias de segurança e processos de recuperação;

V - contas "*Break the glass*" testadas e armazenadas de maneira segura para recuperação do ambiente em cenários de falhas ou desastres;

VI - monitoração do ambiente em relação à qualidade dos serviços;

VII - identificação e classificação das cargas de trabalho e aplicações críticas;

VIII - definição de processo para identificar, triar e endereçar as ameaças e vulnerabilidades de segurança no ciclo de desenvolvimento e de provisionamento dos ambientes;

IX - processos de monitoração dos eventos relacionados à segurança;

X - processos para a segurança e monitoração da conectividade, em especial para os endereços *Internet Protocol* – IP públicos;

XI - critérios para a adoção de criptografia de dados em trânsito e em repouso, com preferência, sempre que tecnicamente viável, pela implementação de criptografia gerenciada pelo cliente; e

XII - definição das áreas requisitantes, bem como dos respectivos serviços, para os quais serão alocados os recursos de *softwares* e de computação em nuvem.

Seção X
Da capacitação no uso de computação em nuvem

Art. 36. A atuação dos servidores e prestadores de serviço terceirizados na operação e no monitoramento dos ambientes de nuvem, bem como no desenvolvimento e na utilização de soluções e serviços em nuvem, exige uma combinação de habilidades técnicas e conhecimentos especializados necessários a garantir a segurança e a performance planejada.

Art. 37. São desejáveis as seguintes competências, em lista exemplificativa e variável para cada tipo de atuação:

I - conhecimentos gerais: compreensão dos conceitos fundamentais de computação em nuvem, incluindo modelos de serviço (IaaS, PaaS, SaaS), tipos de

nuvem (pública, de governo, privada, híbrida) e arquiteturas de nuvem;

II - domínio de plataformas de nuvem: experiência prática com plataformas de nuvem líderes de mercado, especialmente os provedores de serviços em nuvem previstos em contratos firmados pela Polícia Federal, utilizando-se ou não do mecanismo de *cloud broker*;

III - habilidades em virtualização e *containers*: familiaridade com tecnologias de virtualização e experiência em gerenciamento de contêineres;

IV - automatização e orquestração: capacidade de automatizar processos e tarefas repetitivas usando ferramentas de mercado e habilidade para orquestrar recursos em nuvem de forma eficiente;

V - segurança em nuvem: conhecimento em práticas de segurança em nuvem, incluindo controle de acesso, criptografia, monitoramento de segurança, conformidade, gerenciamento de identidade, resposta a incidente e análise forense digital;

VI - gestão de dados: experiência em gerenciamento e engenharia de dados em nuvem, incluindo armazenamento, bancos de dados, migração de dados e implementação de estratégias de cópias de segurança e respectivos processos de recuperação;

VII - desenvolvimento de aplicações em nuvem: habilidades de desenvolvimento de *software* para criar, implantar e escalar aplicações na nuvem, utilizando linguagens de programação;

VIII - monitoramento e otimização de desempenho e de custo: capacidade de monitorar o desempenho dos recursos e custos em nuvem, identificar gargalos e otimizar a utilização de recursos para maximizar a eficiência e reduzir gastos; e

IX - resolução de problemas e tro*ubleshooting*: aptidão para diagnosticar e resolver problemas complexos em ambientes de nuvem, incluindo rede, segurança, desempenho e integração de sistemas.

Seção XI
Da portabilidade e interoperabilidade

Art. 38. A estratégia de desenvolvimento e sustentação de soluções que utilizam a tecnologia de computação em nuvem na Polícia Federal deve garantir flexibilidade e integração entre plataformas e serviços, em nuvem ou não, permitindo a continuidade da prestação do serviço.

Art. 39. Serão adotadas as seguintes medidas práticas com o objetivo de promover a portabilidade e interoperabilidade de sistemas e dados:

I - padrões abertos: serão priorizadas soluções baseadas em padrões abertos, a fim de facilitar a migração entre diferentes provedores de nuvem;

II - ferramentas de migração: serão priorizadas a utilização de ferramentas e serviços de migração a fim de facilitar a transferência de aplicativos e dados entre ambientes de nuvem;

III - monitoramento e gestão unificada: deverá ser fomentado o uso de ferramentas de monitoramento e gestão que possam abranger múltiplos ambientes de nuvem; e

IV - estratégia híbrida: uso das infraestruturas *on-premises* para aumento da disponibilidade, balanceamento de carga ou como site *backup*.

Seção XII
Dos requisitos regulatórios e de conformidade

Art. 40. A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, 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 Agente de Nuvem (*cloud broker)*, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

Art. 41. As soluções de computação em nuvem devem obedecer aos requisitos regulatórios e de conformidade estabelecidos pelos órgãos competentes.

Seção XIII
Da indicação da estratégia de saída

Art. 42. Devem ser previstas estratégias de retorno das cargas de trabalho em nuvem para o ambiente *on-premise* que considerem os seguintes aspectos:

I - uso de serviços e funcionalidades proprietários de provedores de serviços de computação em nuvem;

II - dependências entre sistemas, aplicativos e dados na nuvem;

III - interconexões e integrações críticas que possam impactar a migração de volta ao *on-premise*;

IV - portabilidade das soluções e dados armazenados na nuvem, considerando padrões abertos e evitando bloqueios em virtude de fornecedores;

V - utilização de ferramentas de migração e de cópias de segurança que suportem a transferência eficiente de dados entre a nuvem e o ambiente local;

VI - cópias de segurança completas e atualizados de todos os dados e sistemas na nuvem; e

VII - estratégias de recuperação de desastres para garantir a integridade dos dados, a disponibilidade dos serviços e a continuidade do negócio.

Seção XIV
Da análise de riscos

Art. 43. Uso de *Software* e de Serviços de Computação em Nuvem deve ser precedido de análise dos seguintes fatores de risco:

I - análise dos custos, cenários de escalabilidade, mecanismos de gestão, de modo a garantir previsibilidade e mitigação de riscos orçamentários durante todo o ciclo de vida da solução;

II - acesso não autorizado ou não identificado aos dados da Polícia Federal pelo provedor de serviços;

III - aprisionamento Tecnológico (*lock-in*): dependência excessiva de um provedor de nuvem específico devido à integração profunda de sistemas, dados e serviços. Mitiga-se o risco com a adoção do modelo *multicloud*, evitando um único fornecedor de nuvem, bem como utilizar padrões abertos e arquiteturas flexíveis para facilitar a migração e a integração entre provedores;

IV - catástrofes e desastres naturais: a tecnologia em nuvem oferece uma proteção valiosa contra catástrofes naturais, permitindo redundância geográfica, cópias de segurança automatizadas e recuperação rápida de dados e sistemas. Sua escalabilidade flexível permite uma resposta ágil a situações de emergência, enquanto a colaboração remota e as medidas de segurança reforçadas garantem a continuidade das operações mesmo durante crises. Ao adotar soluções em nuvem, as organizações fortalecem sua resiliência, mitigando os danos causados por desastres naturais e garantindo a segurança e a disponibilidade dos dados; e

V - custo de oportunidade: o custo de oportunidade de não adotar a tecnologia em nuvem e de não aproveitar as soluções tecnológicas mais inovadoras disponíveis no mercado pode ser significativo para a Polícia Federal. Ao optar por permanecer com infraestruturas tradicionais ou soluções desatualizadas, as instituições correm o risco de ficarem para trás na oferta de soluções ao cidadão. A falta de adoção da nuvem pode resultar em custos operacionais mais elevados devido à manutenção de infraestrutura local, além de limitar a agilidade e flexibilidade necessárias para se adaptar às demandas.

Art. 44. A Polícia Federal deverá manter atualizado o mapeamento de riscos para novas contratações de *software* ou de serviços de computação em nuvem.

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

Art. 45. A Polícia Federal adotará, no que for aplicável à estratégia de uso de *software* e computação em nuvem, as obrigações estabelecidas nas leis e normativos vigentes.

CAPÍTULO VI
DA REVISÃO E ATUALIZAÇÃO

Art. 46. Esta estratégia bem como 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 Polícia Federal, quando considerada necessária pelo Comitê Governança Digital.

Art. 47. 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 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 influenciem o uso seguro da computação em nuvem.

CAPÍTULO VII
DAS DISPOSIÇÕES FINAIS

Art. 48. As novas contratações de *software* e serviços de computação em nuvem devem observar as diretrizes apresentadas neste Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal, bem como o modelo de contratação de *software* e de serviços de computação em nuvem.

Art. 49. 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. 50. A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

Art. 51. Os casos omissos não abordados neste Documento de Estratégia de Uso de *Software* e de Serviços de Computação em Nuvem da Polícia Federal serão analisados pelo Comitê de Governança Digital.