30505887 08000.015419/2022-91

Boletim de Serviço em 31/01/2025

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

RESOLUÇÃO CGDSIC/STI/SE/MJSP Nº 27, DE 12 DE DEZEMBRO DE 2024

Aprova o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Ministério da Justiça e Segurança Pública.

O COMITÊ DE GOVERNANÇA DIGITAL E SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO (CGDSIC) do MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA, no uso das atribuições que lhe foram conferidas pelo inciso VIII do art. 2º e pelo art. 6º do Anexo VII da Portaria nº 2, de 28 de janeiro de 2022, do Ministério da Justiça e Segurança Pública, CONSIDERANDO o resultado da deliberação realizada na 6ª Reunião extraordinária do Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC, ocorrida em 12 de dezembro de 2024,

RESOLVE:

Art. 1º Fica aprovado, na forma do Anexo Único desta Resolução, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem do Ministério da Justiça e Segurança Pública - MJSP.

Art. 2º É autorizado o tratamento de dados em ambiente de nuvem pública para viabilizar a prestação de serviços públicos e a implementação de políticas públicas de competência do MJSP, inclusive no caso de dados com restrição de acesso por força de dispositivos legais. Parágrafo único. No tratamento de informações em ambiente de nuvem pública deverão sempre ser observados os instrumentos legais, de governança e de segurança da informação presentes nesta Estratégia.

Art. 3º Esta Resolução entra em vigor na data de sua publicação.

SOLANGE BERTO DE MEDEIROS

Presidente do Comitê de Governança Digital e Segurança da Informação e Comunicação

Documento assinado eletronicamente por **Solange Berto de Medeiros**, **Presidente do Comitê de Governança Digital e Segurança da Informação e Comunicação**, em 31/01/2025, às 19:04, com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

ANEXO ÚNICO
ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

1. DISPOSIÇÕES GERAIS

Este documento tem o objetivo de estabelecer as diretrizes e princípios para o uso de softwares e de serviços de computação em nuvem no Ministério da Justiça e Segurança Pública – MJSP, consolidando os fundamentos de governança necessários para a definição das estratégias e para a tomada de decisões sobre o uso de tecnologias inovadoras para a modernização e a maior eficiência no exercício das atribuições institucionais.

A elaboração da presente estratégia visa atender ao disposto no item 5.5 do Anexo da PORTARIA SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023 e no Art. 4º da INSTRUÇÃO NORMATIVA GSI/PR Nº 5, DE 30 DE AGOSTO DE 2021, e está em conformidade com a Política de Segurança da Informação do MJSP contida na PORTARIA MJSP Nº 2, DE 28 DE JANEIRO DE 2022.

O MJSP, desta forma, estabelece um framework abrangente para orientar a adoção, implementação e gestão responsável de soluções baseadas em softwares e serviços de computação em nuvem, garantindo a integridade dos dados, a proteção da informação sensível e o cumprimento das normas relativas à privacidade e à segurança da informação.

Para o cumprimento dos objetivos estratégicos do MJSP, a instituição busca obter conhecimento a partir de dados e informações gerados por seus processos de negócio ou disponibilizados por outras instituições públicas e privadas. Nos últimos anos, o volume de dados tratados em âmbito institucional aumentou substancialmente, principalmente em razão das diversas competências atribuídas ao órgão, como a gestão de ativos realizada pela Secretaria Nacional de Políticas sobre Drogas, a expansão do uso de plataformas digitais voltadas à prestação de serviços, tais como o sistema Consumidor.gov e os aplicativos Sinesp Cidadão e Celular Seguro, e ainda a grande expansão do tratamento de dados orientados a políticas na área de segurança pública, entre outras necessidades.

A oferta de soluções de cloud computing baseadas em Plataforma como Serviço (PaaS), Infraestrutura como Serviço (IaaS) e Software como Serviço (SaaS) está possibilitando uma revolução no aproveitamento da tecnologia, permitindo acelerar a inovação e prover melhores serviços públicos com aumento da governança e da conformidade, e ainda possibilitando maior economia de recursos.

Portanto, este Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem busca consolidar o interesse do MJSP em utilizar, sempre que for viável sob as óticas técnica, econômica e normativa, a tecnologia de computação em nuvem para o tratamento de seus dados, bem como detalhar os modelos de governança, os papéis e respectivas competências na operação dos ambientes de nuvem do MJSP e os requisitos operacionais e de segurança da informação.

2. OBJETIVOS E COMPETÊNCIAS

São estes os principais objetivos a serem alcançados com a utilização de softwares e da tecnologia de computação em nuvem no MJSP:

• Maior controle e administração sobre os custos com armazenamento e processamento de dados e soluções do MJSP;

• Agilidade e escalabilidade para armazenar e processar dados de interesse da instituição;

• Melhorar a performance e a disponibilidade das plataformas de análise de dados do MJSP;

• Reduzir o intervalo de tempo entre a disponibilização de novidades tecnológicas pelo mercado e a sua efetiva utilização pelo MJSP, principalmente aquelas relacionadas a inteligência artificial;

• Proporcionar o desenvolvimento e a sustentação de soluções disruptivas que possibilitem elevar a produtividade dos processos de trabalho internos.

São estas as competências relacionadas à implementação da estratégia de uso de softwares e de serviços de nuvem no MJSP:

• Ao Comitê de Governança Digital e Segurança da Informação e Comunicação - CGDSIC compete definir e aprovar a Estratégia de Uso de Software e de Serviços de Computação em Nuvem do MJSP, e estabelecer os projetos no âmbito do Plano Diretor de TIC que poderão fazer uso de recursos de softwares e de nuvem;

• À Subsecretaria de Tecnologia da Informação - STI compete aplicar os princípios de governança estabelecidos pelo CGDSIC na gestão dos serviços, buscando realizar o melhor uso da tecnologia para atingir os objetivos institucionais, e ainda por zelar pelo uso racional dos recursos públicos na contratação e no provisionamento de softwares e de recursos de computação em nuvem destinados a atender as necessidades de negócio.

O CGDSIC tem as suas competências estabelecidas no Anexo VII da Portaria nº 02/2022- MJSP, estando entre elas “promover a integração entre as estratégias organizacionais e as estratégias da área de TIC”, “estabelecer diretrizes de alinhamento entre soluções de TIC, a Estratégia de Governo Digital - EGD e o planejamento estratégico do Ministério” e “estabelecer as políticas de minimização de riscos, de priorização e distribuição dos recursos orçamentários de TIC”.

3. DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

3.1. IDENTIFICAÇÃO DAS NECESSIDADES DE NEGÓCIO

As principais necessidades de negócio a impulsionar a contratação de softwares e serviços de computação em nuvem por parte do MJSP estão elencadas a seguir:

• Segurança da Informação e Gerenciamento de Ativos - soluções para análise e correlação de eventos de segurança e resposta a incidentes, incremento da visibilidade de ativos e gestão de riscos para workloads em ambientes multicloud e on premises e capacidade de implementar soluções de segurança da informação e de auditoria com ciclos de vida mais adequados às necessidades institucionais;

• Análise e Ciência de Dados - mecanismos de processamento de grandes volumes de dados, construção de pipelines de processamento batch e em tempo real, engenharia e ciência de dados, entrega de produtos e soluções orientadas a dados para os diferentes clientes internos e externos da instituição;

• Desenvolvimento de Aplicações Modernas e Processos DevOps - possibilidade de construção de soluções de software mais ágeis e escaláveis pelo uso de novas tecnologias e paradigmas como a metodologia DevOps, a programação low-code, tecnologias baseadas em containers e kubernetes, computação serverless e arquitetura de microsserviços orientada a eventos (event-driven), com o objetivo de prover à instituição serviços mais efetivos, de maior escala e em menor prazo;

• Serviços de IA, Aprendizado de Máquina e Computação Cognitiva - APIs e serviços de inteligência artificial e aprendizado de máquina para processamento e enriquecimento de conteúdo de texto, voz, vídeo, imagens e dados georreferenciados e plataformas de desenvolvimento de recursos de machine learning e de IA generativa, potencializando a capacidade da instituição de obter insights e inteligência a partir dos seus dados;

• Infraestrutura, Contingência de Aplicações e Recuperação de Desastres - uso da capacidade disponibilizada pela nuvem para provisionar itens de infraestrutura necessários para a operacionalização de diferentes projetos e ainda para a replicação e/ou backup de dados e aplicações, com o intuito de

melhor responder a situações de desastres que impactem a capacidade de prestação de serviços, aprimorando as práticas de gestão de riscos no que se refere aos serviços de TIC.

• Produtividade e Colaboração – soluções baseadas em SaaS para produção de informações e colaboração por parte dos servidores da instituição por meio de documentos de texto, planilhas, apresentações e dashboards analíticos, ferramentas para comunicação em texto e voz, para constituição de bases de documentos e para publicidade de informações dentro do âmbito institucional.

Em relação ao licenciamento de softwares independentemente do uso em infraestrutura de nuvem pública, dar-se-á preferência ao modelo de subscrição. O licenciamento de softwares pelo mecanismo de marketplace dos provedores de nuvem será considerado excepcional e limitado ao regramento e jurisprudência recentes. Nos casos de necessidade de utilização de softwares com licenciamento específico em ambiente de nuvem, será preferencialmente realizada a modalidade de licença própria do contratante (BYOL – Bring your LIcense).

As definições da presente Estratégia são plenamente aplicáveis ao licenciamento individual de soluções que usam, total ou parcialmente, o modelo de Software como Serviço (SaaS), cabendo neste caso todas as definições relativas ao armazenamento de dados e à segurança da informação aplicáveis à Infraestrutura como Serviço e Plataforma como Serviço fornecidos por meio da nuvem pública.

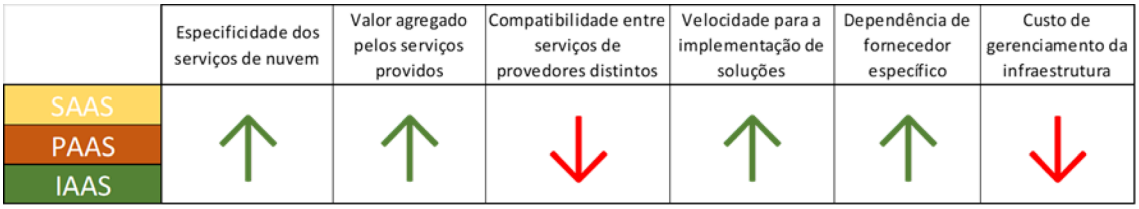
3.2. SELEÇÃO DOS MODELOS

O Ministério da Justiça e Segurança Pública vem utilizando serviços de computação em nuvem desde o ano de 2018, data do primeiro contrato de serviços. Houve um grande aumento do nível de maturidade desde a contratação original, levando ao cenário atual no qual existem diversos projetos sustentados em nuvem, com a utilização de mais de 50 categorias de serviços (por exemplo, máquinas virtuais, bancos de dados, gerenciadores de API etc.) diferentes.

Dentre todas as categorias de necessidades de computação em nuvem apresentadas na seção anterior, apenas para as demandas da categoria “Infraestrutura, Contingência de Aplicações e Recuperação de Desastres” é prevista a utilização expressiva de componentes de Infraestrutura como Serviço. Para todas as demais necessidades a expectativa é que sejam atendidas principalmente por meio de itens de Plataforma como Serviço e Software como Serviço, serviços estes que tendem a ser muito mais específicos de cada provedor de computação em nuvem.

Os serviços IaaS são aqueles que muitas organizações inicialmente procuram quando propõem a migração dos seus workloads de datacenters on premises para a nuvem, porém pode haver muito maior vantagem técnica quando é feita a opção pelo uso de serviços PaaS e SaaS.

O gráfico abaixo ilustra como certos aspectos relacionados ao uso de serviços de computação em nuvem varia em relação à pilha IaaS, PaaS e SaaS:



No gráfico acima, a direção das setas aponta para o sentido de aumento da grandeza indicada. Portanto, na medida em que se escala a pilha IaaS - PaaS - SaaS os serviços providos, de maneira geral, ficam mais específicos, reduz se a compatibilidade com serviços de outros provedores e aumenta-se a dependência de um provedor específico, porém o valor agregado pelos serviços aumenta substancialmente, a velocidade de implementação das soluções é dramaticamente acelerada, e o custo (complexidade) de gerenciamento da infraestrutura reduz sensivelmente. De forma complementar, serviços particulares requerem uma capacitação técnica mais específica das equipes, ou seja, na medida em que se escala a pilha a noção de que existe um conhecimento absolutamente "generalista" aplicável a qualquer serviço de nuvem acaba não sendo verificado na prática. Na realidade, mesmo quando se trata puramente de Infraestrutura como Serviço, existem diferenças sensíveis nos stacks implementados pelos provedores de

nuvem que podem chegar a inviabilizar determinados projetos caso a escolha do provedor seja feita sem a preocupação necessária com os critérios técnicos envolvidos.

Portanto, a ideia aqui apresentada é a de que, em linhas gerais, a utilização de serviços de maior valor agregado PaaS e SaaS pode implicar em maior dependência de fornecedor específico e em maior risco de lock-in, porém traz ganhos indiscutíveis relacionados com a capacidade de implementar soluções complexas e de alto valor negocial em prazo exíguo, de uma forma que, pelos meios tradicionais de desenvolvimento de software e de alocação de infraestrutura no modelo on premises, é praticamente inviável.

A estratégia do MJSP no que diz respeito aos modelos de uso de softwares e de serviços de computação em nuvem é a de buscar os provedores de serviços que apresentem a maior vantagem técnica e econômica para a maior parte do espectro de serviços requeridos e utilizar ao máximo as ofertas de serviços dos provedores contratados, levando ainda em consideração os projetos já existentes na instituição que fazem uso bem-sucedido de soluções PaaS e SaaS em nuvem e o alto valor que esses serviços têm agregado para os objetivos institucionais.

As tecnologias baseadas nas nuvens públicas são altamente necessárias no âmbito dos projetos institucionais para a entrega de valor e de resultados, levando em consideração os aspectos de custo, prazo e qualidade e abrangência dos recursos, razão pela qual são atualmente indispensáveis. Deve ser considerado ainda que alguns recursos que se constituem no “estado da arte” da tecnologia e que são demandados em projetos institucionais, como, por exemplo, as plataformas de desenvolvimento em nível empresarial de soluções baseadas em Inteligência Artificial Generativa de larga escala, somente são acessíveis atualmente por meio de contratos de serviços de nuvem pública.

O MJSP possui uma infraestrutura com datacenters próprios e no momento está executando ações no sentido de modernizar e atualizar tecnologicamente essa infraestrutura. Isso ocorre pelo entendimento de que os serviços de nuvem pública não são vantajosos ou adequados em 100% dos casos, seja em função do custo, seja em função de outros critérios como a autonomia operacional e a localidade dos dados, e que permanece a necessidade de provimento de determinados serviços em infraestrutura própria, até mesmo considerando a preservação dos investimentos já realizados. Ainda assim, os serviços de nuvem pública são considerados essenciais para o cumprimento da missão institucional do órgão, razão pela qual o MJSP vislumbra a sua coexistência com os serviços providos a partir de datacenter próprio, em uma arquitetura de nuvem privada e, eventualmente, híbrida.

Por fim, esta Estratégia estabelece como princípio a utilização prioritária dos serviços de computação em nuvem para as aplicações “cloud ready”, ou seja, aquelas cujo design é particularmente adequado ao provisionamento em nuvem, tais como aplicações baseadas em containers e kubernetes ou aplicações do tipo “event driven”, para as quais há grande vantagem técnica na utilização dos princípios de arquitetura e de implantação em escala propiciados pela nuvem. Não faz parte da estratégia do MJSP a mera transferência máquinas virtuais de aplicações legadas para a nuvem segundo a abordagem lift and shift, considerando inclusive a manutenção de recursos em datacenter próprio para esse fim, sendo admitida essa ação apenas em casos pontuais.

3.3. AVALIAÇÃO DOS POSSÍVEIS FORNECEDORES

No Ministério da Justiça e Segurança Pública são utilizados atualmente serviços de nuvem pública de dois provedores, Microsoft Azure e Oracle Cloud Infrastructure (OCI), sendo estes os provedores considerados os mais aderentes pelos critérios técnicos para os casos de uso da instituição. O Microsoft Azure é a nuvem mais adotada pelo MJSP em decorrência das possibilidades de integrações e da potencialização do uso de outras ferramentas já largamente utilizadas, como no caso das soluções que compõem o pacote Office 365 (Outlook, Sharepoint, Teams, Onedrive, etc), da plataforma de identidades Microsoft Entra e da solução de segurança da informação Microsoft Defender. O MJSP adota também a Oracle Cloud (OCI) principalmente em função da utilização de soluções de gerenciamento de bancos de dados (SGBD) proprietários da empresa em diferentes aplicações corporativas, como é o caso da plataforma Consumidor.gov. Além disso, deve ser destacada a experiência das equipes técnicas da STI/MJSP com os

serviços destas duas nuvens, o que possibilitou a implementação e sustentação de diferentes projetos e o atendimento de diversos casos de negócio.

Eventualmente podem ser considerados os serviços de outros provedores de nuvem pública hyperscale, em especial aquelas empresas que cumpram os requisitos de alta disponibilidade e de presença no território brasileiro (pelo menos uma região completa em território nacional com ao menos três zonas de disponibilidade). Além das já mencionadas Microsoft Azure e Oracle Cloud, atendem a esse requisito os provedores Amazon Web Services (AWS), Google Cloud e IBM Cloud, sendo que destes os quatro primeiros ocupam a posição de líderes no último “quadrante mágico” de “Serviços Estratégicos de Plataforma de Cloud” publicado pelo Gartner em outubro de 2023.

Para a obtenção dos serviços de nuvem pública dos provedores considerados a abordagem preferencial é a de realização de processos licitatórios amplos e transparentes, com a participação irrestrita de parceiros de comercialização dos serviços de cada uma das nuvens públicas, visando a obtenção dos melhores preços para a administração. A contratação de serviços prestados por empresas públicas por meio de outras modalidades de contratação, como a dispensa de licitação, é admita quando for demonstrada a vantagem técnica e econômica desta abordagem, em conformidade com as definições do Acórdão 2233/2020-TCU/Plenário.

3.4. APRISIONAMENTO TECNOLÓGICO E RISCOS DE DEPENDÊNCIA DE FORNECEDOR

A respeito da possibilidade de lock-in com provedores específicos de serviços de nuvem pública, é interessante verificar os apontamentos realizados pelo Gartner Group, organismo que atua com aconselhamento imparcial em Tecnologia da Informação, no documento "Addressing Lock-In Concerns With Public Cloud Infrastructure as a Service" ("Lidando com questões de lock-in em infraestrutura de nuvem pública como um serviço"):

> Principais desafios
>
> **A infraestrutura de nuvem como serviço (IaaS) não é uma commodity. Mesmo no nível de recursos de infraestrutura básica, diferentes provedores usam diferentes conceitos e abstrações.** É relativamente fácil mover imagens de máquina virtual (VM) ou contêiner de sistema operacional de um provedor para outro, mas é muito mais complexo e difícil configurar adequadamente os ambientes de aplicativos de maneira segura, confiável e econômica, pois as práticas recomendadas são diferentes para cada provedor. **A maioria dos clientes usará mais de um provedor de IaaS em nuvem e escolherá o melhor provedor para cada aplicativo. Embora um desses provedores provavelmente seja o provedor estratégico principal, os clientes**

> **devem investir no gerenciamento de todos esses provedores de nuvem diferentes, da mesma forma que investem no gerenciamento de diferentes sistemas operacionais (SOs) e pilhas de aplicativos.**
>
> O mercado se consolidou em torno de dois líderes de mercado, Amazon Web Services (AWS) e Microsoft Azure, com um terceiro concorrente significativo no Google Cloud Platform (GCP). Todos os três têm serviços altamente diferenciados que abrangem o espectro de IaaS a plataforma como serviço (PaaS). Os clientes obtêm o maior valor da adoção de serviços "up the stack" e do uso dessas ofertas IaaS e PaaS (IaaS + PaaS) integradas como um todo, resultando em aprisionamento.
>
> Recomendações
>
> Os líderes de arquitetura corporativa e inovação tecnológica com responsabilidade pela estratégia de nuvem devem:
>
> **Construir sua arquitetura para portabilidade de aplicativos, não portabilidade de infraestrutura.**
>
> **Identifique seus motivadores mais importantes para a portabilidade de aplicativos e tome decisões pragmáticas de arquitetura em uma base de aplicativo por aplicativo. Identifique todos os riscos sistêmicos criados pela dependência de um determinado provedor de nuvem.**
>
> **Abraçar toda a gama de ofertas do seu provedor de nuvem para maximizar o valor do seu investimento.** Compreenda o valor derivado e os desafios de negócios associados criados por pontos de lock-in, para gerenciar os riscos e equilibrá-los em relação aos benefícios.
>
> Quando a portabilidade é uma prioridade, busque a independência contextual, com dependências facilmente satisfeitas e interfaces bem definidas. Certifiquese de ter planos de contingência para os piores cenários.

A mensagem transmitida pelo Gartner para as organizações que buscam formas de evitar o lock-in no emprego de soluções de computação em nuvem pode ser resumida em alguns pontos principais: tenha, se possível, mais de um provedor de nuvem como alternativa; utilize tudo o que o seu provedor é capaz de fornecer (incluindo ofertas PaaS) para maximizar o seu retorno; busque construir aplicações que sejam portáveis entre provedores; crie estratégias para mitigar os riscos de lock-in e de interrupção de negócios.

Conforme apontado pelo Gartner, uma “estratégia multinuvem” é desejável para evitar o risco de aprisionamento tecnológico, mas também aponta quando é benéfico às organizações decidir pela multiplicidade de provedores de nuvem, considerando as heterogeneidades e os custos inerentes ao gerenciamento de diferentes plataformas, conforme o documento “How to Decide Between a Single-Cloud or Multi-cloud Strategy” (Como decidir entre uma estratégia de cloud única ou multicloud). Alguns dos apontamentos do trabalho são reproduzidos abaixo:

> Os profissionais técnicos com função de arquiteto de nuvem devem fornecer orientação para colocar cargas de trabalho em nuvem em IaaS e PaaS em nuvem. **Para evitar o gerenciamento e a governança caóticos em uma estratégia multicloud, pelo menos um provedor deve ser designado como o local preferido para cargas de trabalho em nuvem.**
>
> As organizações que estabelecem uma estratégia multicloud para infraestrutura como serviço (IaaS), plataforma como serviço (PaaS) ou IaaS e PaaS integrados (IaaS+PaaS) também devem estabelecer orientações firmes sobre quando usar um provedor de nuvem em vez de outro. **Caso contrário, as cargas de trabalho serão espalhadas arbitrariamente por vários provedores de nuvem, resultando em desafios com a integração de aplicativos e dados, além de aumento da complexidade operacional e dos custos relacionados à rede e à segurança.**
>
> A maioria das organizações escolhe uma estratégia multicloud de longo prazo para ampliar o acesso a capacidades diferenciadas e pode perceber que isso reduz os riscos relacionados ao fornecedor. **A maioria escolherá um fornecedor estratégico primário, que servirá como sede de pelo menos 70% das cargas de trabalho e provavelmente será inicialmente o único fornecedor.**
>
> Para simplificar a governança e a gestão e reduzir os desafios de integração de dados, a **maioria das organizações limitará estritamente a utilização de fornecedores adicionais a cenários que não podem ser servidos através de um dos fornecedores preferenciais.**

De forma geral, a estratégia seguida pelo MJSP para mitigar os riscos de aprisionamento tecnológico vem sendo a recomendada pelo Gartner, buscando construir estruturas de aplicação baseadas em tecnologias (em especial containers e kubernetes) que possam ser portadas entre diferentes provedores e até mesmo para sua infraestrutura própria, porém sem desprezar a oferta de serviços PaaS de alta relevância para os projetos institucionais. Em relação ao uso de múltiplas nuvens, o cenário de dois provedores mais nuvem privada própria tem se mostrado adequado para mitigar o risco excessivo de lockin para a maioria dos

casos, devendo ser considerado, no entanto, a existência de certos workloads para os quais há maior dependência de um provedor específico, o que é de certa forma inevitável quando considerado o valor agregado aos projetos por certas tecnologias exclusivas. Nesse cenário, o MJSP somente vislumbra a utilização de outros provedores nos casos em que os atuais não apresentarem soluções técnica ou economicamente viáveis para futuras necessidades institucionais.

3.5. SEGURANÇA DA INFORMAÇÃO

Os provedores de serviços de nuvem públicas deverão ser todos integralmente aderentes às disposições da Instrução Normativa nº 05/2021 - DSIC/GSI, que trata dos requisitos de segurança da informação para a prestação de serviços de computação em nuvem para entidades da Administração Pública Federal.

Em particular, os instrumentos contratuais deverão conter todos os dispositivos relativos à segurança da informação previstos no Art. 19 da referida norma, quais sejam:

> I - termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do órgão ou da entidade para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;
>
> II - garantia da exclusividade de direitos, por parte do órgão ou da entidade, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;
>
> III - proibição do uso de informações do órgão ou da entidade pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;
>
> IV - conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;
>
> V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem aos órgãos ou às entidades contratantes ao término do contrato;
>
> VI - eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do órgão ou entidade sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados; e
>
> VII - garantia do direito ao esquecimento para dados pessoais, conforme art. 16 da Lei nº 13.709, de 14 de agosto de 2018 - LGPD.

Por fim, os contratos deverão prever a obrigação das empresas contratadas para o fornecimento de serviços de nuvem de apresentar, previamente ao início da prestação de serviços, os relatórios de tipos I e II da auditoria SOC 2, em conformidade com a previsão existente no art. 25 da IN nº 05/2021. A apresentação destes relatórios deverá ser condição necessária o início da execução da ordem de serviços e para o consumo dos recursos de nuvem do provedor contratado.

Os provedores deverão ser ainda aderentes a padrões de organismos internacionais como ISO/IEC, AICPA (certificação SOC 2), PCI SSC (certificação PCI-DSS), NIST (certificação FIPS), dentre outras, como forma de atestar a conformidade das suas operações com as mais rígidas práticas de segurança da informação.

É obrigação das equipes técnicas gerenciadas pela STI/MJSP aplicar as melhores práticas disponibilizadas pelos provedores de nuvem para a proteção da informação, como a adoção de controles de acesso em nível de rede (Firewall, IPS, WAF, AntiDDoS etc.), o uso de mecanismos para garantir a segurança na gestão de identidades, o uso de autenticação multifator sempre que possível e o uso obrigatório de criptografia para os dados em repouso e os que forem acessados por meio de aplicações e APIs. A implantação destes e de outros controles para a segurança da informação e a privacidade de dados pessoais é escopo do Programa de Privacidade e Segurança da Informação (PPSI), iniciativa da Secretaria de Governo Digital do Ministério da Gestão e Integração (SGD/MGI) para aumentar a maturidade dos órgãos governamentais nesses assuntos, e tais controles são plenamente aplicáveis também no caso dos workloads implantados em nuvem.

A Instrução Normativa nº 05/2021-DSIC/GSI estabelece ainda obrigações relativas à residência dos dados armazenados em nuvens públicas. De acordo com a norma, dados com restrição de acesso por consequência de leis e de normas infralegais deverão ser necessariamente armazenados em datacenters dos provedores de nuvem localizados em território nacional, e que dados sem restrição de acesso podem

ser armazenados de forma irrestrita na nuvem, inclusive em data centers fora do Brasil, desde que mantendo uma cópia de segurança em datacenter do provedor localizado em território nacional.

Por sua vez, a Portaria nº 5.950/2023-MGI reforça essas restrições e estabelece ainda, no item 5.4.2 do seu Anexo, a necessidade de autorização da instância de governança de TIC do órgão (papel desempenhado pelo CGDSIC no caso do MJSP) como condição para o armazenamento de dados com restrição de acesso em nuvem pública, e que preferencialmente tais dados devem ser armazenados em "nuvem de governo", conceituada na Portaria como uma nuvem privada dotada de autonomia operacional e gerenciada por órgão ou empresa pública.

A estratégia proposta para o MJSP contempla as duas possibilidades, o armazenamento de dados restritos na sua própria nuvem privada de governo implantada em seus datacenters ou em datacenters gerenciados por empresas públicas e o uso de nuvem pública nos casos em que os ganhos com o uso das tecnologias próprias existentes nas nuvens públicas justifiquem o tratamento de dados nesses ambientes. Para o segundo caso, no entanto, estão previstas medidas adicionais de governança para dar garantias à área de TIC e à área negocial responsável pelo projeto de que as melhores práticas relativas à conformidade com as leis e normas e relativas à segurança da informação estão sendo seguidas.

A previsão de utilização de nuvem de governo para o tratamento de dados de segurança pública visa ainda evitar o enquadramento das restrições legais impostas pelo art. 3º, § 4º da Lei 13.709/2018 (LGPD).

A conformidade das ações aqui propostas passa pela aprovação deste documento por parte do CGDSIC/MJSP, como forma de atender ao disposto no item 5.4.2 do Anexo da Portaria nº 5.950/2023-MGI.

Por fim, e em observância ao disposto no Art. 17, II, da Instrução Normativa nº 05/2021- DSIC/GSI, é vedado tratamento em ambiente de computação em nuvem de informações classificadas em grau de sigilo (reservadas, secretas e ultrassecretas), nos termos do Decreto nº 7.724, de 16 de maio de 2012, assim como documentos preparatórios que possam originar informação classificada em grau de sigilo.

3.6. PROCESSOS DE GOVERNANÇA NA UTILIZAÇÃO DE SERVIÇOS DE NUVEM E SOFTWARES

O Ministério da Justiça e Segurança Pública, para a prestação diferentes serviços e políticas públicas que estão em sua esfera de competência, necessita realizar o tratamento de fontes de dados que possuem restrição de acesso em função de diferentes dispositivos legais e, em especial, realizar o tratamento de dados referentes a pessoas naturais protegidos pela Lei nº 13.709/2018 (Lei Geral de Proteção de Dados).

Considerando essa realidade, a sua Subsecretaria de Tecnologia da Informação vem realizando ações no sentido de catalogar e classificar as fontes de dados tratadas por seus processos e workloads. Esse é um processo em constante evolução e aprimoramento, e que vem sendo constantemente ampliado em decorrência da expansão da oferta de serviços e aplicações por parte da Subsecretaria.

Nos casos em que o tratamento de dados é realizado em ambiente de nuvem pública, além da observância de todos os limites e restrições já elencados, é de vital importância que haja aceite e concordância formal por parte da área negocial responsável pelos serviços e/ou políticas públicas a serem suportados. Desta forma, o modelo de governança aqui proposto prevê o estabelecimento de um "Plano de Implantação de Serviços em Nuvem" a ser firmado para cada projeto que envolva o tratamento de dados em ambiente de nuvem pública, sejam esses dados com ou sem restrição de acesso, de forma a caracterizar o compromisso e o compartilhamento de responsabilidades entre as áreas negocial e técnica sobre a decisão de suportar os workloads em nuvem. O documento deverá descrever em detalhes o propósito da implantação, as necessidades de negócio que busca atender, os recursos tecnológicos que deverão ser fornecidos, as fontes de dados a serem tratadas e a sua classificação, os resultados a serem atingidos e o custo estimado do projeto, em alinhamento com as definições do item 7 e subitens do Anexo da Portaria nº 5.950/2023-MGI.

Outra disciplina relevante e que merece ser ressaltada é a de gestão dos custos de nuvem, custos estes que podem variar significativamente em função das abordagens tecnológicas dos projetos a serem implementados e que necessitam ser mantidos sob estrito controle, sob pena de gerar gastos elevados e/ou não vinculados a resultados. A equipe de fiscalização de contratos de nuvem deve ter a capacidade

de acompanhar tais custos e realizar as intervenções necessárias para a sua previsibilidade no longo termo, ainda que, em situações específicas, seja necessário um maior provisionamento de recursos em decorrência de uma demanda pontual ou sazonal. O eventual gasto adicional em um determinado período deverá ser consignado ao longo do processo de fiscalização, sendo responsabilidade da equipe técnica de TIC propor alternativas para reequilibrar o consumo de recursos caso necessário, visando a manutenção do saldo necessário para atendimento de todas as necessidades institucionais até o término da vigência. Este exercício de engenharia financeira, ou "FinOps", no jargão próprio dos serviços de computação em nuvem, é condição necessária e essencial para uma boa gestão dos contratos desta natureza, e é uma competência que deve ser adquirida pelos servidores responsáveis pela fiscalização e gestão contratual.

3.7. ALINHAMENTO COM NORMAS E POLÍTICAS INSTITUCIONAIS

A presente "Estratégia de Uso de Softwares e de Computação em Nuvem" está alinhada com o planejamento de TIC vigente e com as políticas institucionais de segurança da informação. Cita-se abaixo exemplo relacionado à nova contratação referente aos serviços de nuvem do MJSP, conforme demonstrado abaixo:

Plano Diretor de TI (PDTI):

- Ação A0446 – Aquisição de Serviços de Nuvem Microsoft Azure;
- Ação A0447 – Contratação de Serviços de Nuvem Oracle e Cloud at Customer.

Plano de Contratações Anual (PCA):

- DFD 67/2024 - Contratação de serviço de computação em nuvem

Política de Segurança da Informação do MJSP, publicada pela Portaria MJSP nº 02, de 28 de janeiro de 2022:

> *Da Computação em Nuvem*
>
> *Art. 36. Fica permitido o tratamento das informações em ambiente de computação em nuvem, considerando a legislação vigente e os riscos de segurança da informação e comunicação.*
>
> *§ 1º O tratamento das informações deve ser realizado em ambiente previamente homologado pela autoridade da área de Tecnologia da Informação e Comunicação.*
>
> *§ 2º É vedado o tratamento, em ambiente de computação em nuvem, de informação classificada em grau de sigilo, conforme a legislação vigente.*
>
> *Art. 37. Nas contratações de soluções de tecnologias da informação e comunicação que utilizem recursos de computação em nuvem, devem ser observados os regramentos e as legislações vigentes que tratam do armazenamento de dados, metadados, inclusive as cópias de segurança quanto à necessidade de permanência em território nacional.*
>
> *Parágrafo único. A área de Tecnologia da Informação e Comunicação deve manter monitoramento visando garantir que o disposto no caput deste artigo seja cumprido.*

3.8. RECURSOS INSTITUCIONAIS NECESSÁRIOS PARA A OPERAÇÃO DE SOFTWARES E SERVIÇOS DE COMPUTAÇÃO EM NUVEM

A Subsecretaria de TI do Ministério da Justiça e Segurança Pública vem, ao longo do tempo, ampliando seu grau de maturidade no processo de gestão de serviços de licenciamento de softwares e de computação em nuvem. No entanto, ações adicionais seguem sendo necessárias e deverão ser planejadas, por exemplo, para a maior capacitação de pessoal dedicado às atividades de fiscalização e gestão contratual, tais como a capacitação específica em processos de gerenciamento de custos (FinOps) e de governança de serviços em nuvem.

Outra ação considerada necessária é o reforço de pessoal e uma estrutura organizacional mais adequada às responsabilidades advindas da gestão de serviços de nuvem. Em relação a esse tópico, já existe uma proposta de reformulação do organograma da STI sendo discutida no Ministério da Gestão e Integração, sendo essas tratativas de responsabilidade da Secretaria Executiva do MJSP.

No que diz respeito aos serviços profissionais necessários para a sustentação de workloads em nuvem, a STI/MJSP atua neste momento para reformular o seu contrato de serviços de suporte aos usuários e à infraestrutura de TIC, de modo a incluir disciplinas e capacitações específicas dedicadas ao melhor uso e aproveitamento das tecnologias disponibilizadas pelos provedores de nuvem. Além desta iniciativa, a STI/MJSP conta com a manutenção de outros contratos dedicados ao suporte e apoio à sustentação de serviços em nuvem, como o contrato de serviços de suporte Unified celebrado com a Microsoft.

Em relação aos serviços profissionais necessários para o monitoramento de segurança da informação da infraestrutura de TIC on premisse e em nuvem do MJSP, o órgão possui contratos de SOC (Security Operation Center) e ferramental especializado, além de equipe técnica dedicada para sustentar os processos de segurança da informação.

Por fim, em relação aos recursos de infraestrutura física, tais como a conectividade de rede necessária para o uso de serviços em nuvem, a STI/MJSP conta atualmente com contratos que fornecem acesso redundante e independente à internet, porém planeja incluir em sua próxima contratação de serviços de nuvem solução de conectividade dedicada à interligação da sua sede e centro de dados com os provedores por meio de enlaces de alta capacidade e baixa latência.

4. NORMA DE USO SEGURO DE COMPUTAÇÃO EM NUVEM

As definições existentes na presente Estratégia de Uso de Software e de Serviços de Computação em Nuvem atendem integralmente ao disposto nos Arts. 4º e 5º da Instrução Normativa nº 05/2021-DSIC/GSI, que tratam da necessidade de um ato normativo regulamentando o uso seguro de computação em nuvem, garantindo, portanto, a conformidade com este requisito normativo.

5. ORIENTAÇÕES PARA O USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM E/OU SOFTWARES PARA CESSÕES, DOAÇÕES E REPASSES A ENTES FEDERATIVOS

Quando a solução e/ou software adquirido destinar-se a cessões, doações e afins aos Entes Federativos, caberá à Administração Pública Federal orientar o usuário/destinatário acerca de cuidados específicos, visando a segurança da informação, a privacidade e a conformidade com a legislação aplicável. Estes cuidados incluem, entre outros:

I. Avaliação da Relevância e Necessidade: orientar o usuário a avaliar periodicamente a real necessidade da solução ou software, considerando se as funcionalidades atendem de fato suas necessidades.

II. Configurações de Segurança Inicial: recomendar a utilização de configurações padronizadas de segurança, como credenciais de acesso, senhas, multifator de autenticação e permissões de usuários, para mitigar riscos de segurança.

III. Treinamento e Capacitação: proporcionar treinamento adequado ao usuário final acerca das funcionalidades da solução e/ou software, destacando aspectos de segurança, boas práticas de uso e como reportar eventuais incidentes.

IV. Políticas de Privacidade e Proteção de Dados: reforçar a importância do cumprimento das políticas de privacidade e proteção de dados pessoais, conforme disposto na Lei Geral de Proteção de Dados (LGPD), incluindo a necessidade de consentimento para o tratamento de dados sensíveis.

V. Monitoramento e Auditoria: sugerir a implementação de práticas regulares de monitoramento e auditoria das atividades realizadas nas soluções e softwares, a fim de garantir a integridade das informações e a conformidade com as diretrizes de segurança adotadas.

VI. Resposta a Incidentes: orientar os usuários sobre a necessidade de reporte à Administração Pública Federal (cedente) acerca de irregularidades, com diretrizes claras para identificação, resposta e mitigação

de incidentes relacionados ao uso da solução.

VII. Encaminhamento de Dúvidas e Suporte: disponibilizar um canal de atendimento ao usuário para esclarecimento de dúvidas e necessidade de suporte técnico, assegurando um atendimento eficaz no momento de implantação e uso da solução.

VIII. Descarte Seguro de Dados: fornecer instruções claras sobre a forma adequada de descarte de dados e informações armazenadas na solução ou software, garantindo que todos os dados pessoais ou sensíveis sejam eliminados de maneira segura, conforme legislação vigente.

Essas orientações visam garantir que todos os usuários das soluções e softwares, independentemente de seu vínculo com a administração pública federal, estejam cientes das responsabilidades e melhores práticas para assegurar a efetividade e a segurança na utilização das ferramentas proporcionadas.

6. DISPOSIÇÕES FINAIS

Em atenção ao disposto no Art. 6º da Instrução Normativa nº 05/2021-DSIC/GSI, a comissão constituída para a elaboração da presente Estratégia deverá ser responsável pela sua revisão periódica, processo que deverá ocorrer em prazo não superior a dois anos da sua aprovação.