Visão Multivigente

RESOLUÇÃO CTSI/RFB Nº 3, DE 14 DE JUNHO DE 2024

(Publicado(a) no Boletim de Serviço da RFB de 14/06/2024, seção 1, página 6)

Aprova o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem da Secretaria Especial da Receita Federal do Brasil.

A PRESIDENTE DO COMITÊ DE TECNOLOGIA E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA ESPECIAL DA RECEITA FEDERAL DO BRASIL, no uso das competências que lhe conferem as Portarias RFB nº 800 e 801, ambas de 28 de junho de 2013, e considerando a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, a Resolução CTSI/RFB nº 1, de 16 de março de 2020, e o resultado da 1ª Reunião Ordinária do Comitê de Tecnologia e Segurança da Informação do exercício de 2024, realizada em 24 de maio 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 da Secretaria Especial da Receita Federal do Brasil (RFB).

Art. 2º Devem ser mantidas em ambiente de nuvem de governo, cargas de trabalho que tratem informação com restrição de acesso prevista na legislação, como as 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.

§ 1º A Coordenação-Geral de Tecnologia e Segurança da Informação (Cotec) avaliará a viabilidade técnica das soluções de nuvem de governo oferecidas no momento do planejamento, desenvolvimento ou implantação dos projetos que forem autorizados a utilizar a tecnologia da computação em nuvem.

§ 2º Caso a tecnologia de nuvem de governo oferecida aos projetos não atenda ao que se busca com as suas respectivas entregas, poderão ser usadas nuvens públicas e suas soluções e serviços (nativos ou não) para desenvolver e sustentar soluções de tecnologia, inclusive com a hospedagem e o processamento de informação com restrição de acesso prevista na legislação.

§ 3º As diretrizes de governança, segurança, controle de acesso, definição de perfis de acesso e as condições mínimas de infraestrutura do ambiente informatizado da RFB são válidas, no que se aplicar, ao ambiente de nuvem.

Art. 3º Esta Resolução entra em vigor na data de sua publicação no Boletim de Serviço da RFB.

ADRIANA GOMES REGO

ANEXO ÚNICO

DOCUMENTO DE ESTRATÉGIA DE USO DE SOFTWARE E DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

1. DISPOSIÇÕES GERAIS

Tendo em vista o disposto na PORTARIA SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023, na INSTRUÇÃO NORMATIVA GSI/PR Nº 5, DE 30 DE AGOSTO DE 2021, e na RESOLUÇÃO

CTSI/RFB nº 1, DE 16 DE MARÇO DE 2020, este documento traz as diretrizes e princípios para o uso de software e de serviços de computação em nuvem na Receita Federal do Brasil (RFB), refletindo o compromisso da instituição com a modernização e eficiência de suas operações por meio da adoção estratégica de tecnologias inovadoras.

Com a crescente complexidade das operações tributárias e a demanda por maior agilidade, segurança e conformidade, a tecnologia de computação em nuvem emerge como uma prioridade estratégica para a RFB. Este documento visa estabelecer uma estrutura abrangente para orientar a adoção, implementação e gestão responsável de serviços e soluções baseadas em nuvem, garantindo a integridade dos dados, a proteção da informação sensível e o cumprimento das regulamentações tributárias e de segurança da informação. Ao alinhar a governança de nuvem com os objetivos estratégicos da RFB, espera-se promover uma administração tributária mais ágil, eficiente e transparente, capacitada a atender às crescentes demandas da sociedade e do ambiente digital em constante evolução.

O DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020 estabeleceu, dentre as estratégias do governo digital, adotar tecnologia de processos e serviços governamentais em nuvem como parte da estrutura tecnológica dos serviços e setores da administração pública federal. Um componente crítico para o cumprimento dos objetivos estratégicos da RFB é a habilidade de obter conhecimento a partir de toda a informação disponível. Nos últimos anos, o volume de dados disponível aumentou substancialmente, principalmente devido ao grande volume de documentos eletrônicos recebidos do Sistema Público de Escrituração Digital (SPED).

Nos últimos anos, os serviços de Plataforma como Serviço (PaaS) e Infraestrutura como Serviço (IaaS) oferecidos pelas principais empresas fornecedoras – públicas e privadas – de nuvem estão possibilitando uma revolução na utilização da tecnologia, permitindo um melhor ritmo de inovação, mais velocidade e agilidade, melhor governança, maior conformidade, além de mais eficiência e economia de custos.

Portanto, este Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem busca reafirmar o compromisso da RFB em utilizar massivamente a tecnologia de computação em nuvem para o armazenamento e o processamento de seus dados e suas soluções, bem como detalhar a governança, os papéis e respectivas competências na operação dos ambientes de nuvem da RFB, requisitos de operação e segurança, e a política de uso de dados e cargas de trabalho que tratem informação com restrição de acesso prevista em legislação específica.

2. OBJETIVOS, COMPETÊNCIAS E NECESSIDADES DE NEGÓCIO

São estes os principais objetivos e necessidades de negócio a serem alcançados com a utilização da tecnologia de computação em nuvem na RFB:

• Maior controle e administração sobre os custos com armazenamento e processamento de dados e soluções da RFB;

• Agilidade e escalabilidade para armazenar e processar dados de interesse econômico fiscal;

• Melhorar a performance e a disponibilidade do ambiente analítico da RFB.

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

• Proporcionar o desenvolvimento e a sustentação de soluções que suportem processos de trabalho modificados em virtude de reformas fiscais estruturantes; e

• Proporcionar o desenvolvimento e a sustentação de soluções disruptivas que possibilitem a alavancagem da produtividade em processos de trabalho internos e/ou ofertas de serviço ao contribuinte.

São estas as competências relacionadas à implementação da estratégia de nuvem na RFB:

• Ao Comitê de Tecnologia e Segurança da Informação (CTSI) compete definir a estratégia de nuvem para a RFB, bem como o orçamento anual a ser aplicado em soluções em nuvem da RFB.

• À Cotec compete realizar a governança dos componentes de nuvem conforme diretrizes definidas pelo CTSI, bem como as atividades relativas:

o Ao gerenciamento de componentes de desenvolvimento;

o Ao gerenciamento de componentes de plataformas de desenvolvimento interno;

o Ao gerenciamento de soluções de inteligência artificial e demais recursos relacionados; e

o Ao gerenciamento dos orçamentos de projetos e ambientes, nos casos de previstos na estratégia de uso de nuvem.

o Ao gerenciamento de componentes de infraestrutura/operação; e

o Ao gerenciamento de componentes de segurança.

o Ao gerenciamento de componentes do ambiente analítico em nuvem.

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

a) Seleção dos modelos adequados:

A Receita Federal do Brasil, a partir dos estudos realizados (fato descrito e analisado no tópico “b” deste documento), entende que a adoção da computação em nuvem é uma premissa do órgão para avançar na melhoria dos processos de trabalho e na oferta de serviços ao cidadão.

Para tal, a RFB, alinhada ao disposto no item 5.4.3 do Anexo I da PORTARIA SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023, entende que:

1. Devem ser mantidas em ambiente de nuvem de governo 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;

2. A Cotec avaliará a viabilidade técnica das soluções de nuvem de governo oferecidas no momento do planejamento, desenvolvimento ou implantação dos projetos que forem autorizados a utilizar a tecnologia da computação em nuvem;

3. Caso a tecnologia de nuvem de governo oferecida aos projetos não atenda ao que se busca com as suas respectivas entregas, poderão ser usadas nuvens públicas e suas soluções e serviços (nativos ou não) para desenvolver e sustentar soluções de tecnologia, inclusive com a hospedagem e o processamento de informação com restrição de acesso prevista na legislação;

4. Os projetos desenvolvidos ou em desenvolvimento que se enquadrem no item anterior deverão ser aprovados pelo CTSI antes de sua entrada em produção ou antes do início do desenvolvimento quando houver a necessidade de manipulação de informação com restrição de acesso prevista na legislação;

5. Para o caso de provas de conceito e projetos-piloto, a Cotec poderá autorizar, em ato conjunto com a Coordenação-Geral 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.

b) Avaliação dos possíveis fornecedores:

O quadrante mágico do Gartner (série de relatórios de pesquisa de mercado publicados pela empresa de consultoria de TI Gartner que se baseiam em métodos proprietários de análise de dados qualitativos para demonstrar tendências de mercado, como direção, maturidade e participantes) para infraestrutura na nuvem como serviço possibilita a identificação de três empresas

que mais se destacam nos quesitos “habilidade em execução” e “completude da visão”. As empresas que se destacam são:

• Amazon Web Services (AWS);

• Google; e

• Microsoft.

A partir de dezembro de 2020, por intermédio das NT COTEC 58/2020 e 38/2021, foi instituída uma prova de conceito (POC) com o objetivo de medir a performance de serviços ofertados pelas nuvens como IaaS e PaaS comparando-os com o Receita Data.

Os testes realizados possibilitaram:

• Medir o tempo de execução de programa que simula o processo de transformação dos dados e geração de tabelas.

• Realizar consultas analíticas por meio de comandos específicos sobre as tabelas geradas, medindo o desempenho (duração da consulta) em diversas condições.

• Realizar o processamento de muitas expressões regulares sobre um fluxo contínuo de conteúdo, gerando um fluxo de saída com as indicações de quais expressões foram satisfeitas sobre quais documentos.

• Executar testes sobre performance de recursos computacionais aplicando implementações próprias e de terceiros.

• Executar testes em geral, comparando os resultados de uma implementação própria com as soluções ofertadas pelos provedores.

• Executar testes de segurança com o objetivo de avaliar os riscos do armazenamento de dados protegidos pelo sigilo fiscal em uma nuvem.

Os resultados dos testes demonstram que:

• As nuvens oferecem diversas opções de recursos computacionais possibilitando a contratação gradual, podendo atender a vários sistemas que se encontram com demandas reprimidas para ambientes de produção com um custo inferior ao cobrado pelo Serpro nos serviços de hosting (hospedagem de soluções e aplicações)

• Em diversos testes as nuvens são mais rápidas que o serviço hosting oferecido pelo Serpro.

• Os testes com processamento de imagens demonstraram que as nuvens oferecem ótima performance e possibilidade de adições e reduções de acordo com nossa necessidade. Isto atende à crescente demanda da RFB por este tipo de processamento sem a necessidade de uma contratação inicial superdimensionada.

Por fim, ficou demostrado na oportunidade da POC que a Google, Microsoft e Amazon alcançaram as metas definidas, igualando ou superando a performance do Receita Data e dos serviços de hosting contratados com o Serpro, demonstrando inequivocamente a viabilidade técnica de substituir o Receita Data por soluções em nuvem, bem como a hospedagem de soluções estruturantes. Ressalta-se: como já mencionado, na oportunidade da POC foram avaliados os três maiores provedores de nuvem daquele momento. Caso surja necessidade de adotar novo provedor de nuvem não avaliado inicialmente, será realizado procedimento de avaliação similar para verificar se eles também atendem aos requisitos estabelecidos pela RFB.

Mais recentemente, as principais empresas públicas de tecnologia da informação no Governo Federal – Serpro e Dataprev – lançaram as suas soluções de nuvens privadas (ou de governo), que se utilizam do serviço “cloud stack”, firmando parcerias com as principais empresas provedoras de nuvem para oferecer recursos de nuvem hospedados nos seus datacenters.

c) Requisitos mínimos de segurança:

• Deverá ser adotado, sempre que cabível, os controles e medidas definidos no Programa de Privacidade e Segurança da Informação. Os controles e medidas mínimos necessários serão definidos conforme a avaliação de criticidade de cada sistema;

• A não implementação de um controle ou medida cabível deve ser feito tendo como base uma avaliação de risco prévia;

• Sempre que possível, os recursos de sistemas deverão ser segmentados. De modo a evitar que uma falha ou incidente de segurança cibernético, impacte outros sistemas;

• 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;

• As aplicações e as cargas de trabalho devem implementar controles para detectar e proteger a exfiltração de dados; e

• Cargas de trabalho e aplicações deverão executar periodicamente scan de vulnerabilidade em todos os recursos.

d) Política de governança:

Política de governança de nuvem deverá ser estabelecida conjuntamente pelas áreas responsáveis pela governança e gestão da operação em nuvem, que deverá respeitar as seguintes diretrizes relacionadas à resiliência e segurança:

• Cargas de trabalho e aplicações deverão ter métricas definidas para avaliar a confiabilidade do serviço;

• De acordo com a criticidade da carga de trabalho, planejar a arquitetura e requisitos de resiliência a falhas, além do plano para “Disaster Recovery”;

• Provedores de identidade devem ter alta disponibilidade;

• Implementar mecanismos de segurança nas cargas de trabalho e aplicações: WAF, Firewall, DDoS, etc;

• Gestão segura de certificados, chaves e segredos, garantindo backup e redundância;

• Contas “Break the glass” testadas e armazenadas de maneira segura para recuperação do ambiente em cenários de falhas ou desastres;

• Monitorar ambiente em relação a qualidade dos serviços;

• Identificar e classificar as cargas de trabalho e aplicações críticas;

• Definir processo para identificar, triar e endereçar as ameaças e vulnerabilidades de segurança no ciclo de desenvolvimento;

• Estabelecer processo de monitoração dos eventos relacionados à segurança;

• Definir processos para a segurança de conectividade em especial para os endereços de IP públicos; e

• Definir critérios para se adotar criptografia dos dados em trânsito e em repouso.

e) Diretrizes de uso seguro de software e de serviços de computação em nuvem:

O uso de softwares na nuvem está sujeito aos mesmos controles e restrições aplicadas a softwares instalados em computadores da RFB, devendo passar pelo processo de homologação ou autorização, mesmo que em rito simplificado. O uso de 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 ao serviço.

A coordenação responsável por cada sistema ou carga de trabalho da RFB deve, com o apoio da Coordenação de Tecnologia, avaliar se o sistema ou carga de trabalho pode ser migrado para a nuvem, considerando os normativos de segurança da informação e tratamento de informações em nuvem aplicáveis. A Coordenação responsável deverá elaborar também uma

análise de risco como parte do planejamento da migração de sistemas e cargas de trabalho para o ambiente de nuvem.

f) Diretrizes de governança e condições mínimas de infraestrutura de TIC do órgão ou entidade para utilizar serviços de computação em nuvem:

As diretrizes de governança e as condições mínimas de infraestrutura do ambiente informatizado da RFB para recursos da rede interna e hospedados em prestadores de serviços são válidas, no que se aplicar, ao ambiente de nuvem. Os controles e parâmetros aplicados aos atores organizacionais da RFB, tais como controle de acesso, definição de perfis de acesso e outros, devem ser aplicados também ao ambiente de produção em nuvem.

g) Princípios norteadores da estratégia:

Levando em conta as diretrizes estratégicas da RFB, bem como os normativos que regem o tema, alguns princípios norteadores são essenciais, quais sejam:

• Cloud-First: Com base no DECRETO Nº 10.332, DE 28 DE ABRIL DE 2020, este princípio preconiza que, sempre que possível, as soluções e serviços devem ser concebidos e implementados na nuvem. Isso implica em aproveitar ao máximo os benefícios intrínsecos da escalabilidade, flexibilidade e agilidade oferecidos pelos provedores de serviços em nuvem.

• Uso de Broker Multicloud: Reconhecendo a diversidade e a complexidade do ecossistema de nuvem, o uso de um "Broker Multicloud" permite aproveitar o melhor de cada provedor de serviços em nuvem, escolhendo soluções específicas que atendam melhor às necessidades técnicas, regulatórias e de custo. Além disso, o modelo de "Broker Multicloud" oferece redundância e resiliência, minimizando os riscos de dependência excessiva de um único provedor.

• Priorização da Segurança: a segurança permanece como uma prioridade fundamental. 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. Busca-se mitigar os riscos cibernéticos e proteger ativos mais valiosos, especialmente os dados, contra ameaças internas e externas.

• Capacitação Contínua: Será preconizado um investimento contínuo em capacitação e desenvolvimento de competências técnicas. A RFB deve promover uma cultura de inovação e colaboração, incentivando a experimentação e o aprendizado contínuo.

h) Alinhamento com outros planos estratégicos e estabelecimento de linhas de base e metas de benefícios/resultados esperados:

Os projetos e ações relacionados ao uso de computação em nuvem na RFB deverão estar alinhados às diretrizes estratégicas da instituição, bem como ao Plano Diretor de Tecnologia da Informação (PDTI). Outrossim, novas soluções a serem contratadas junto a fornecedores e provedores de nuvem deverão constar no Plano de Contratações Anual (PCA).

O uso da computação em nuvem na RFB busca, além dos objetivos já presentes nesse documento, 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.

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 preferencialmente 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 RFB.

i) Considerações sobre capacitação da equipe do órgão ou entidade que gerenciará, operará ou utilizará os recursos de software e de computação de serviços em nuvem, identificando as capacidades e habilidades necessárias;

A atuação dos servidores da RFB 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. São desejáveis os seguintes conhecimentos, em lista exemplificativa e variável para cada tipo de atuação:

• Conhecimentos Gerais: compreensão dos conceitos fundamentais de computação em nuvem, incluindo modelos de serviço (IaaS, PaaS, SaaS), tipos de nuvem (pública, privada, híbrida) e arquiteturas de nuvem.

• 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 RFB, utilizando-se ou não do mecanismo de cloud broker.

• Habilidades em Virtualização e Containers: familiaridade com tecnologias de virtualização e experiência em gerenciamento de contêineres.

• Automatização e Orquestração: capacidade de automatizar processos e tarefas repetitivas usando ferramentas de mercado, e habilidade para orquestrar recursos em nuvem de forma eficiente.

• 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 forense digital.

• Gestão de Dados: experiência em gerenciamento de dados em nuvem, incluindo armazenamento, bancos de dados, migração de dados e implementação de estratégias de backup e recuperação.

• Desenvolvimento de Aplicações em Nuvem: habilidades de desenvolvimento de software para criar, implantar e escalar aplicações na nuvem, utilizando linguagens de programação.

• Monitoramento e Otimização de Desempenho: capacidade de monitorar o desempenho dos recursos em nuvem, identificar gargalos e otimizar a utilização de recursos para maximizar a eficiência e reduzir custos.

• Resolução de Problemas e Troubleshooting: aptidão para diagnosticar e resolver problemas complexos em ambientes de nuvem, incluindo rede, segurança, desempenho e integração de sistemas.

j) Considerações sobre portabilidade e interoperabilidade entre sistemas, dados e serviços, bem como a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor;

A estratégia de desenvolvimento e sustentação de soluções que utilizam a tecnologia de computação em nuvem na RFB deve garantir flexibilidade e integração entre plataformas e serviços, em nuvem ou não, a fim de garantir continuidade da prestação do serviço e fluidez. Estas são as medidas práticas a serem consideradas e que promovem a portabilidade e interoperabilidade de sistemas e dados, buscando reduzir qualquer tipo de dependência de um único provedor de nuvem:

• Padrões Abertos: Serão priorizadas soluções baseadas em padrões abertos, a fim de facilitar a migração entre diferentes provedores de nuvem.

• Estratégia Multicloud: Deverá ser adotada uma estratégia de multicloud, distribuindo cargas de trabalho entre diferentes provedores de nuvem público ou privado, aproveitando o melhor que cada provedor tem a oferecer, reduzindo risco de dependência, considerando o custo de transferência de dados entre provedores de nuvem.

• 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.

• Monitoramento e Gestão Unificada: Deverá ser fomentado o uso de ferramentas de monitoramento e gestão que possam abranger múltiplos ambientes de nuvem.

k) Requisitos regulatórios e de conformidade;

As soluções de computação em nuvem na RFB devem obedecer aos requisitos regulatórios e de conformidade estabelecidos pelos órgãos competentes, inclusive aos requisitos

estabelecidos pelos órgãos de controle interno e externo, especialmente aos normativos em vigor ora estabelecidos, quais sejam:

• PORTARIA SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023, que estabelece modelo de contratação de software e de serviços de 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;

• 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; e

• RESOLUÇÃO CTSI/RFB nº 1, DE 16 DE MARÇO DE 2020, que autoriza hospedagem, em nuvem pública, das soluções informatizadas da RFB.

l) Indicação da Estratégia de Saída, considerando a análise de dependências e aspectos de portabilidade:

A migração de serviços e dados para a nuvem é normalmente acompanhada pela necessidade de flexibilidade e escalabilidade. No entanto, circunstâncias podem surgir, como mudanças nas políticas de segurança, custos ou requisitos regulatórios, que levam à consideração do retorno para o modelo tradicional de armazenamento e hospedagem de dados e soluções. Para tal, a estratégia de nuvem da RFB considera ao menos as seguintes ações:

• Análise de Dependências:

o Dependências entre sistemas, aplicativos e dados na nuvem.

o Interconexões críticas que possam impactar a migração de volta ao on-premise.

• Avaliação de Portabilidade:

o Portabilidade das soluções e dados armazenados na nuvem, considerando padrões abertos e evitando bloqueios em virtude de fornecedores.

o Utilização de ferramentas de migração e backup que suportem a transferência eficiente de dados entre a nuvem e o ambiente local.

• Backup e Recuperação:

o Backups completos e atualizados de todos os dados e sistemas na nuvem.

o Estratégias de recuperação de desastres para garantir a integridade dos dados durante o retorno ao on-premise.

m) Análise de riscos:

Os riscos de utilização de uma solução tecnológica de computação em nuvem na RFB foram avaliados na NT COTEC 035/2021 seguindo o Modelo de Gestão de Riscos da RFB (probabilidade, impacto, controles existentes, controles propostos e risco residual) com a classificação "Média".

A referida Nota Técnica evidencia que “todas as soluções testadas na prova de conceito apresentaram elementos de segurança considerados indispensáveis pela RFB”. Foram analisados os seguintes riscos:

• Acesso não identificado aos dados da RFB pelo provedor de serviços, com a consequente quebra da confidencialidade dos dados e até do sigilo fiscal.

• Ampliação dos pontos de contato com a internet, que podem ser aproveitados para ataques à RFB e, consequentemente, indisponibilização de serviços ou roubos de dados

Além dos pontos acima mencionados, complementa-se o mapeamento anterior com os seguintes riscos e as respectivas ações de mitigação acerca da hospedagem de dados em nuvem:

• Risco de Aprisionamento Tecnológico (lock-in): o aprisionamento tecnológico, ou lock-in, é um risco significativo associado à adoção de serviços em nuvem. Refere-se à 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.

• Risco de Catástrofes e Desastres Naturais: a tecnologia em nuvem oferece uma proteção valiosa contra catástrofes naturais, permitindo redundância geográfica, backups automatizados 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.

• Risco do 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 RFB. 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. Além disso, ao não aproveitar as soluções tecnológicas mais inovadoras, as instituições podem perder oportunidades de melhorar a eficiência operacional e impulsionar a produtividade das equipes. O custo de oportunidade de não adotar a tecnologia em nuvem e não aproveitar as soluções mais avançadas pode resultar em uma posição institucional

A RFB deverá realizar novo mapeamento de riscos para novas contratações de software ou de serviços de computação em nuvem observando o disposto no item 23.3.2 do Anexo I da Portaria SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023, ou a qualquer tempo.

APÊNDICE

DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Deverão ser observados os requisitos mínimos deste capítulo para que a RFB adote soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia. Este capítulo cumpre com as obrigações presentes na Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021.

A) Da transferência de serviços para um provedor de serviço de nuvem

Antes de transferir serviços ou informações para um provedor de serviço de nuvem, a RFB deverá:

I - garantir que estejam alinhadas à legislação brasileira, aos direitos à privacidade, à proteção dos dados pessoais, as demais normas estabelecidas pela RFB e ao sigilo das comunicações privadas e dos registros as seguintes operações:

a) de coleta, armazenamento, guarda e tratamento de registros de dados pessoais;

b) de comunicações realizada por provedores de conexão e de aplicações de internet, em que pelo menos um desses atos ocorra em território nacional;

II - realizar o gerenciamento de riscos, precedido por análise e relatório de impacto de dados pessoais, em conformidade com a legislação;

III - definir o modelo de serviço e de implementação de computação em nuvem que será adotado;

IV - avaliar quais informações serão hospedadas na nuvem, considerando requisitos presentes nesse documento;

V - definir as medidas de mitigação de riscos e de custos para a implementação de solução de computação em nuvem e para possibilidade de crescimento dessa solução; e

VI - planejar custos de migração das informações e dos serviços, nos casos de ingresso e de saída do serviço de computação em nuvem.

B) Da capacidade do provedor de serviço de nuvem para implementar atualizações

Em função da capacidade do provedor de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a RFB deverá revisar e atualizar periodicamente os processos internos de gestão de riscos de Segurança da Informação.

O provedor de serviço de nuvem deverá possuir uma política de atualização de versão de software, indicando sua criticidade.

C) Do gerenciamento de identidades e de registros (logs)

Em relação ao gerenciamento de identidades e de registros, a RFB deverá:

I - observar a regulamentação estabelecido pela RFB quanto à geração, ao tratamento, à guarda e à recuperação de registros de eventos (log) nas soluções em computação em nuvem, e ao controle de acesso lógico no ambiente informatizado da RFB e tratamento de acesso e dos privilégios dos usuários;

II - negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação da RFB;

III – além do uso de recursos de autenticação que garantam a identificação individual e inequívoca do usuário, quando do acesso aos ativos de informação, adotar, de acordo com o nível de criticidade da informação, o uso da tecnologia single-sign-on, o qual deve ser acompanhado:

a) de autenticação multifator; ou

b) de outra alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem;

IV – exigir do provedor de serviço de nuvem que:

a) registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações; e

b) armazene, pelo período de um ano, todos os registros de que trata a alínea a;

VI - armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por no mínimo cinco anos, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério da RFB;

VII - manter em ambiente próprio controlado, por no mínimo cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem; e

VIII - capacitar a equipe de segurança para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem bem como para avaliar se os controles de segurança e os papéis e permissões atribuídos a cada identidade são adequados às características das cargas de trabalho.

D) Do uso de recursos criptográficos

Em relação à necessidade do uso de recursos criptográficos, a RFB deverá:

I – verificar se os dados da organização estão sendo tratados e armazenados de acordo com a legislação;

II - avaliar a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios; e

III - utilizar, sempre que possível, chaves de encriptação baseadas em hardware.

E) Da segregação de dados e da separação lógica

Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o provedor de nuvem contratado deverá:

I - garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas, devendo haver controles de segurança da informação de

forma a propiciar o isolamento adequado dos recursos utilizados pela RFB dos demais recursos utilizados por usuários do serviço em nuvem pública;

II - garantir que seja aplicada segregação lógica apropriada dos dados das aplicações virtualizadas, dos sistemas operacionais, do armazenamento e da rede a fim de estabelecer a separação de recursos utilizados; e

III - garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela RFB.

Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, RFB deverá:

I – Restringir a superfície de ataque, principalmente externa, das cargas de trabalho à menor possível, evitando expor ativos e serviços diretamente à internet, exceto quando estritamente necessário.

F) Do tratamento da informação

Em relação ao tratamento da informação em ambiente de computação em nuvem, a RFB, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais, deve observar as diretrizes presentes no item 3.a desse Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem:

Os dados, metadados, informações e conhecimentos produzidos ou custodiados pela RFB, transferidos para o provedor de serviço de nuvem, devem estar hospedados em território brasileiro, observando-se as seguintes disposições:

I - pelo menos uma cópia atualizada de segurança deve ser mantida em território brasileiro;

II - a informação sem restrição de acesso poderá possuir cópias atualizadas de segurança fora do território brasileiro, conforme legislação aplicável; e

III - no caso de dados pessoais, deverão ser observadas as orientações previstas na Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais - LGPD, e demais legislações sobre o assunto.

Norma específica da RFB pode autorizar o compartilhamento em nuvem pública de arquivos com usuários externos, inclusive protegidos por sigilo fiscal.