RESOLUÇÃO CGD/IFPR Nº 23, DE 20 DE MAIO DE 2025

Dispõe sobre a estratégia de uso de *software* e de serviços de computação em nuvem no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Paraná (IFPR).

O Presidente do Comitê de Governança Digital do Instituto Federal de Educação, Ciência e Tecnologia do Paraná, no uso de suas atribuições legais, considerando o contido no processo 23411.009872/2025-63,

RESOLVE *AD REFERENDUM*:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS E ESCOPO

Art. 1° Criar a estratégia de uso de *software* e de serviços de computação em nuvem no âmbito do Instituto Federal de Educação, Ciência e Tecnologia do Paraná (IFPR).

Art. 2° Esta estratégia tem o objetivo de assegurar que o IFPR obtenha os resultados esperados e mitigue os riscos associados à adoção de possíveis novas tecnologias ou novas formas de contratação no âmbito do IFPR .

Parágrafo único. A definição de uma estratégia de uso de *software* e serviços de computação em nuvem é uma iniciativa fundamental para alcançar estes objetivos.

Art. 3° Esta estratégia deve ser aplicada para novas contratações de *software* e de serviços de computação em nuvem no âmbito do IFPR, 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;

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

Art. 4° As contratações de *software* e de serviços de computação em nuvem deverão ser realizadas observando-se o processo de contratação de soluções de tecnologia da informação e comunicação disposto pela Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, e o modelo de contratação descrito no Anexo I da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023.

Parágrafo único. Deve-se avaliar a viabilidade de utilização de modelos já adotados na Administração, pois aumenta o nível de padronização nas contratações no âmbito do SISP.

CAPÍTULO II

DAS REFERÊNCIAS

Art. 5º Para o desenvolvimento e aplicação da estratégia de uso de *software* e de serviços de computação em nuvem, cabe ao IFPR observar, sem prejuízo das demais normas em vigor:

I - Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023;

II - Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021;

III - Decreto nº 9.637, de 26 de dezembro de 2018;

IV - Resolução SE/GSI nº 1, de 11 de setembro de 2019;

V - Demais leis, decretos, resoluções, portarias e instruções normativas relacionadas à segurança da informação publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

VI - Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022;

VII - Lei nº 14.133, de 1º de abril de 2021;

VIII - Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021;

IX - Decreto nº 7.724, de 16 de maio de 2012 (Classificação da Informação - LAI);

X - Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação - LAI);

XI - Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD).

CAPÍTULO III

DOS CONCEITOS E DEFINIÇÕES

Art. 6° Para fins de compreensão dos termos utilizados nesta norma, serão considerados os seguintes conceitos e definições, conforme as fontes:

I - Atualização de versões: disponibilização, por parte do fabricante, de uma versão completa ou parcial do *software* com funcionalidades adicionais ou evoluções tecnológicas que compreendam uma nova versão estável do produto, podendo incluir correções.

II - Banco de Dados como Serviço (DBaaS): ambiente no qual o recurso usado pelo órgão ou entidade é um banco de dados disponibilizado e operado pelo provedor de serviços em nuvem, acessado por APIs ou meios equivalentes.

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

IV - Catálogo de Soluções de TIC com condições padronizadas: relação de soluções de TIC ofertadas pelo mercado que possuem condições padrões definidas pelo Órgão Central do SISP.

V - *Cloud Broker* (Integrador de Serviços em Nuvem): realiza a integração dos serviços de computação em nuvem com agregação de valor entre o órgão ou a entidade e dois ou mais provedores. 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, orientado por padrões internacionais e nacionais.

VI - Consultoria especializada em *software*: serviços especializados de configuração, customização, instalação, otimização e manutenção em *software* cujos padrões de desempenho e qualidade podem ser objetivamente definidos no Termo de Referência.

VII - *Data center*: estrutura dedicada à acomodação, interconexão e operação de equipamentos de tecnologia da informação e redes de telecomunicações, fornecendo serviços de armazenamento, processamento e transporte de dados.

VIII - Função como Serviço (FaaS): recursos fornecidos para construir e gerenciar aplicativos de microsserviços ou equivalentes, de forma escalável.

IX - Incidente de Segurança da Informação: qualquer evento de segurança da informação indesejável e inesperado que pode comprometer as operações de negócio e ameaçar a segurança da informação.

X - Instância de Computação: componente de computação em nuvem composto de máquina virtual e serviços agregados (armazenamento, rede, etc.) necessários para sua operação.

XI - Nuvem de governo: infraestrutura de nuvem privada ou comunitária gerida exclusivamente por órgãos ou empresas públicas.

XII - Nuvem híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas) agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade.

XIII - Nuvem privada ou interna: infraestrutura de nuvem dedicada para uso exclusivo do órgão e suas unidades, cuja propriedade pode ser do órgão ou empresas públicas relacionadas a TI. Admite o uso de recursos de provedores de nuvem pública somente se assegurado o isolamento lógico e físico.

XIV - Provedor de serviços em nuvem: empresa que possui infraestrutura de TI destinada ao fornecimento de infraestrutura, plataformas e aplicativos baseados em computação em nuvem.

XV - Região: agrupamento de localizações geográficas específicas onde os recursos computacionais estão hospedados.

XVI - Serviço: meio de entregar valor aos usuários internos ou externos à organização ao facilitar o alcance de resultados.

XVII - Serviços agregados: serviços adicionais providos pelo fornecedor (suporte técnico, treinamento, atualizações, implementação, etc.).

XVIII - Sistemas estruturantes: sistemas de informação para operacionalizar e sustentar atividades de pessoal, orçamento, finanças, etc., comuns a todos os órgãos da Administração, que necessitam de coordenação central.

XIX - *Software* livre: *software* de código aberto que pode ser usado, estudado, modificado e redistribuído gratuitamente sob licença que permite acesso e modificação do código-fonte.

CAPÍTULO IV

DOS PRINCÍPIOS NORTEADORES

Art. 7° Esta estratégia segue os seguintes princípios norteadores:

I - Respeito aos princípios e diretrizes constitucionais, legais e regulamentares que regem a administração pública federal;

II - Garantia de integridade, autenticidade e disponibilidade da informação sob a custódia do IFPR, com respeito ao princípio da transparência e atribuição de confidencialidade apenas nos casos expressamente previstos na legislação;

III - Alinhamento estratégico da Política de Segurança da Informação com os demais planos;

IV - Alinhamento estratégico com a Estratégia de Governo Digital e a Estratégia Brasileira para a Transformação Digital (E-Digital), Ciclo 2022-2026, com o objetivo específico de adotar tecnologia de processos e serviços governamentais em nuvem;

V - *Cloud First*;

VI - *Lift-and-shift* como último recurso (exemplo de princípio);

VII - *Broker multicloud* (exemplo de princípio).

CAPÍTULO V

DOS OBJETIVOS E COMPETÊNCIAS

Art. 8° Os objetivos a serem alcançados com a adoção desta estratégia incluem:

I - Assegurar que o IFPR obtenha os resultados esperados e mitigue os riscos;

II - O melhor uso dos recursos financeiros e humanos na manutenção e expansão das soluções de TI;

III - Alinhamento com a Estratégia de Governo Digital e a Estratégia Brasileira para a Transformação Digital;

IV - Identificação do modelo de implantação de nuvem considerando as características de cada carga de trabalho em relação ao nível de sigilo das informações.

Art. 9° Compete aos seguintes atores organizacionais:

I - Alta Administração: Assegurar a utilização de tecnologias de computação em nuvem em conformidade com este documento; disponibilizar recursos financeiros e humanos para a implementação da estratégia. Aprovar e divulgar atos normativos sobre uso seguro da nuvem.

II - Comitê de Segurança da Informação: Aprovar e revisar atos normativos sobre estratégia e uso seguro; estabelecer países para armazenamento de dados federais; definir requisitos criptográficos mínimos; analisar conclusivamente minutas de atos normativos. Analisar casos omissos.

III - Gestor de Segurança da Informação: Instituir e coordenar equipe para elaboração/revisão de atos normativos; supervisionar aplicação; assegurar comunicação efetiva com provedor sobre controles/SLAs de segurança; propor ações de segurança para implementação/contratação de nuvem.

IV - Diretoria de Tecnologia da Informação e demais setores de TI das unidades do IFPR: Implementar procedimentos relativos ao uso de tecnologias de computação em nuvem conforme este documento e legislação pertinente. Priorizar participação em processos licitatórios centralizados pela SGD/MGI. Especificar serviços de nuvem e levantar fornecedores/preços em alinhamento com as normas. Adequar sistemas/serviços para migração e elaborar plano de retorno.

V - *Cloud Broker* (se aplicável): Realizar a integração dos serviços entre o IFPR e provedores de serviço de nuvem. Apoiar o IFPR em descobrir, planejar, migrar, configurar, utilizar, gerenciar e evoluir os serviços. Garantir que provedores representados cumpram requisitos legais e de segurança. Apresentar relatórios de auditoria SOC 2 (tipo I e II) de todos os provedores que representa.

CAPÍTULO VI

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

Art. 10 O IFPR deverá observar as seguintes diretrizes ao adotar soluções de *software* e computação em nuvem:

I - Identificação das necessidades do negócio: Identificar e avaliar as necessidades antes da contratação. Determinar quais sistemas, aplicações, dados e serviços precisam ser movidos, como serão acessados e quais recursos computacionais e de armazenamento serão necessários.

II - Seleção dos modelos adequados: Avaliar quais modelos de serviço (IaaS, PaaS, SaaS) e de implementação (nuvem pública, nuvem privada, nuvem híbrida, nuvem de governo etc.) melhor se adequam aos requisitos de negócio. A identificação do modelo de implantação deve considerar o nível de sigilo das informações. Cargas de trabalho sem restrição de acesso podem usar qualquer ambiente de nuvem. Cargas de trabalho com informação com restrição de acesso (sigilo fiscal, bancário, etc.) devem ser mantidas em ambiente de nuvem de governo, exceto se autorizado. Sistemas estruturantes devem usar somente nuvem privada ou comunitária restritas às infraestruturas de órgãos/entidades.

III - Estabelecimento de uma política de governança: Assegurar que a política de governança abranja identificação/classificação de dados, controle de acesso, gerenciamento de configuração e monitoramento para garantir conformidade. Definir papéis e responsabilidades para as áreas de TI, de negócio e da nuvem. Elaborar matriz de responsabilidades que inclua obrigações do órgão/entidade.

IV - Diretrizes de uso seguro: Conhecer os normativos sobre segurança da informação e tratamento de informações em nuvem, identificar sistemas/*workloads* migráveis e medidas de gerenciamento de risco para informações sigilosas. Os requisitos mínimos para adoção segura devem ser observados.

V - Avaliação quanto às condições mínimas de infraestrutura de TI: Ter conexão estável com a Internet e com banda suficiente para gerenciar *softwares* e serviços de computação em nuvem.

VI - Alinhamento com outros planos estratégicos: Esta estratégia deve estar alinhada com os Planos Estratégicos Institucionais, Planos de TI, Plano de Contratações Anual (PCA) e Planos de Segurança da Informação. As contratações de *Software* e Serviços de Computação em Nuvem deverão estar explicitamente previstas no PCA. Havendo necessidade de indicação de marca/provedor, explicitá-la no PCA.

VII - Estabelecimento de linhas de base e metas: Definir linhas de base e metas de benefícios/resultados esperados (agilidade, redução de custos, resiliência, segurança). Mapeamento “AS IS” e “TO BE” é um exemplo.

VIII - Considerações sobre capacitação da equipe: Capacitar a equipe que gerenciará, operará ou utilizará os recursos, identificando capacidades e habilidades necessárias.

IX - Considerações sobre portabilidade e interoperabilidade: Considerar a viabilidade de adoção de medidas para mitigar a dependência tecnológica ou aprisionamento ao provedor.

X - Requisitos regulatórios e de conformidade: Considerar os requisitos regulatórios e de conformidade para o uso seguro no âmbito do IFPR e da administração pública federal.

XI - Indicação da estratégia de saída: Considerar a análise de dependências e aspectos de portabilidade (*backup*, redundância, contratos de apoio, retorno para a infraestrutura local etc.). Estabelecer procedimento relacionado à transição e encerramento contratual, incluindo devolução/eliminação/retenção de dados e garantia ao direito ao esquecimento.

XII - Análise de riscos: Considerar as diretrizes de gerenciamento de riscos constantes no modelo de contratação federal. Realizar mapeamento de riscos da contratação (identificação, classificação, tratamento), considerando a realidade organizacional, apetite a risco, impacto em políticas públicas, dependência tecnológica, etc. O risco de volumetria incompatível (sub/superdimensionamento) deve ser considerado.

CAPÍTULO VII

DEFINIÇÃO DOS REQUISITOS PARA O USO SEGURO DE COMPUTAÇÃO EM NUVEM

Art. 11 O IFPR trata os requisitos para uso seguro de computação em nuvem em norma específica para esta finalidade. Devem ser observados os requisitos mínimos da Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021, que incluem, no mínimo:

I - Antes de transferir serviços ou informações para um provedor, garantir que as operações (coleta, armazenamento, tratamento) estejam alinhadas à legislação brasileira, direitos à privacidade, proteção de dados pessoais e sigilo das comunicações.

II - Avaliar riscos de segurança e privacidade ao disponibilizar informações a terceiros.

III - Definir o modelo de serviço e de implementação de computação em nuvem a ser adotado.

IV - Utilizar, para os sistemas estruturantes, somente os modelos de implementação de nuvem privada ou de nuvem comunitária, desde que restritas às infraestruturas de órgãos ou entidades.

V - Avaliar quais informações serão hospedadas na nuvem, considerando a classificação da informação, valor do ativo e controles de acesso.

VI - Manter em ambiente próprio controlado, por 5 anos, registros de acessos, incidentes e eventos cibernéticos.

VII - Capacitar a equipe de segurança para acessar e utilizar os registros do provedor.

VIII - Em relação ao uso de recursos criptográficos: verificar tratamento de dados conforme legislação; analisar necessidade de criptografar com base em requisitos, riscos, criticidade, custos e benefícios; utilizar chaves baseadas em hardware sempre que possível.

IX - Em relação à segregação de dados e separação lógica: garantir que o ambiente contratado seja protegido de usuários externos e não autorizados; implementar controles para isolamento adequado; garantir segregação lógica apropriada de dados, aplicações, sistemas operacionais, armazenamento e rede; garantir separação de recursos do provedor daqueles da administração interna; avaliar riscos de *softwares* proprietários na nuvem.

X - Em relação ao tratamento da informação: observar a legislação sobre proteção de dados pessoais; informações com restrição de acesso, material restrito do órgão, informação pessoal, documentos preparatórios podem ser tratados na nuvem, observando riscos e legislação. Dados custodiados pelo órgão/entidade e transferidos para o provedor devem estar hospedados em território brasileiro.

XI - Em relação às cláusulas contratuais: o contrato deve conter termo de confidencialidade que impeça o uso/transferência/liberação de dados a empresas/governos estrangeiros. Garantir exclusividade de direitos do órgão/entidade sobre as informações tratadas. Prever a devolução/eliminação de dados ao término do contrato. Observar a LGPD.

XII - O provedor de serviço de nuvem deverá possuir metodologia de gestão de riscos conforme as melhores práticas e legislação .

CAPÍTULO VIII

DA GESTÃO CONTRATUAL

Art. 12 Na gestão dos contratos de *software* e serviços de computação em nuvem, o IFPR deverá observar as seguintes diretrizes:

I - Gerenciamento de Custos: Implementar mecanismos fundamentais para assegurar a governança e supervisão na gestão contratual em relação aos limites autorizados de execução dos recursos previstos nas ordens de serviço. Assegurar a estrita observância, para fins de pagamento, aos limites de recursos e serviços estabelecidos em cada ordem de serviço. O gerenciamento de custos deve ser responsabilidade da contratada, conforme diretrizes estabelecidas nas ordens de serviço. Poderá ser avaliada a necessidade de contratação de serviços especializados de auditoria técnica para otimização dos recursos.

II - Vigência dos Contratos: O contrato poderá ter vigência de até 5 anos para serviços contínuos, prorrogável até o limite de 10 anos.

III - Ordens de Serviço (OS): Toda emissão de ordem de serviço deverá ser precedida de levantamento da demanda real dos volumes, considerando necessidades atuais e riscos. Os volumes a constar da OS devem ser precedidos de levantamentos, estimativas e cálculos que justifiquem a demanda. A OS deve conter, no mínimo, objetivo, descrição, produtos/resultados, prazo, e requisitos não funcionais. A equipe de fiscalização deve implementar mecanismos próprios de controle dos volumes consumidos, evitando aferição baseada exclusivamente em relatório da contratada. O pagamento da nota fiscal deve ser condicionado à autorização prévia do gestor do contrato após o Termo de Recebimento Definitivo.

IV - Transição e Encerramento Contratual: Estabelecer procedimento que inclua a obrigação do provedor em efetuar a devolução dos dados, informações e sistemas à contratante, eliminação de dados, retenção de dados conforme legislação e garantia ao direito ao esquecimento para dados pessoais.

V - Governança da Contratação: Incluir na matriz de responsabilidades um registro formal sobre o uso de serviços de nuvem, contendo função, responsável (órgão/entidade ou *cloud broker*) e nível de responsabilidade. No caso de uso de *cloud broker*, prever instrumento contratual acessório que assegure o regime de compartilhamento de responsabilidades entre *broker* e provedor.

CAPÍTULO IX

DA REVISÃO E ATUALIZAÇÃO

Art. 13 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 do IFPR, ou quando considerada necessária pelo Comitê de Segurança da Informação.

Art. 14 Em função da capacidade dos provedores de serviço de computação em nuvem em implementar atualizações relacionadas à segurança da informação, a presente estratégia deve ser revisada em até 2 (dois) anos para:

I - Definir novos critérios e a periodicidade das atualizações dos procedimentos e dos recursos computacionais a serem observados pelo provedor de serviço de nuvem;

II - Atualizar periodicamente os processos internos de gestão de riscos de segurança da informação;

III - Quando ocorrerem eventos, fatores relevantes, novos requisitos tecnológicos, corporativos e/ou legais que exijam sua revisão imediata;

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 X

DAS DISPOSIÇÕES FINAIS

Art. 15 As novas contratações de *software* e serviços de computação em nuvem devem observar as diretrizes apresentadas neste documento, bem como o modelo de contratação de *software* e de serviços de computação em nuvem no âmbito do SISP.

Art. 16 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. 17 A alta administração deve disponibilizar os recursos (humanos, tecnológicos e financeiros) necessários para a execução desta estratégia.

Art. 18 Os casos omissos não abordados neste documento serão analisados pelo Comitê de Segurança da Informação.

Art. 19 Esta Resolução entra em vigor a partir da data de sua publicação.

Documento assinado eletronicamente por **ADRIANO WILLIAN DA SILVA VIANA PEREIRA**, **Reitor**, em 21/05/2025, às 12:15, conforme horário oficial de Brasília, com fundamento no art. 6º, caput, do Decreto nº 8.539, de 8 de outubro de 2015.

A autenticidade deste documento pode ser conferida no site https://sei.ifpr.edu.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **3594905** e o código CRC **A77B6C8D**.

Referência: Processo nº 23411.009872/2025-63 SEI nº 3594905