



FUNDAÇÃO UNIVERSIDADE FEDERAL DE SÃO CARLOS

SECRETARIA GERAL DE INFORMÁTICA - Sin

Rod. Washington Luís km 235 - SP-310, s/n - Bairro Monjolinho, São Carlos/SP, CEP 13565-905

Telefone: (16) 33518147 - <http://www.ufscar.br>

PORTARIA SIN Nº 144/2025

Estabelece a Estratégia de Uso de Software e de Serviços de Computação em Nuvem no âmbito da Universidade Federal de São Carlos (UFSCar)

O Secretário Geral de Informática da UFSCar, no uso das competências que lhe confere o Regimento Interno do Comitê de Governança Digital da UFSCar, aprovado pela [Resolução ConsUni Nº 23, de 07 de março de 2025](#), considerando a necessidade da definição da Estratégia de Uso de Software e de Serviços de Computação em Nuvem da UFSCar nos termos da Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e a deliberação do Comitê de Governança Digital da UFSCar em sua 21ª Reunião Ordinária, ocorrida em 12 de junho de 2025.

RESOLVE:

Art. 1º Fica aprovado, na forma do Anexo Único desta Portaria, o Documento de Estratégia de Uso de Software e de Serviços de Computação em Nuvem da UFSCar.

Art. 2º A área de Tecnologia da Informação da UFSCar, representada pela Secretaria Geral de Informática (Sin), deverá adotar, monitorar e garantir a aplicação das diretrizes estabelecidas nesta Estratégia, visando assegurar a qualidade e a conformidade na utilização dos recursos e nas contratações de software e dos serviços de nuvem, de acordo com as necessidades institucionais.

Art. 3º Esta Portaria entra em vigor na data de sua publicação no Boletim de Serviço Eletrônico do SEI-UFSCar.

ERICK LAZARO MELO

Secretário Geral de Informática

ANEXO Estratégia de Uso de Software e Serviços de Computação em Nuvem da UFSCar

Dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito da Universidade Federal de São Carlos - UFSCar.

1. Introdução e Fundamentação Normativa

A adoção estratégica de softwares e serviços de computação em nuvem é um componente essencial para a modernização e a eficiência da Universidade Federal de São Carlos (UFSCar). Diante da imperativa transformação digital, as soluções em nuvem oferecem a agilidade, escalabilidade e segurança necessárias para otimizar os recursos tecnológicos em conformidade com as demandas institucionais e normativas.

O presente documento formaliza a política para a contratação, gestão e governança de tecnologias em nuvem. Seus objetivos são:

- Orientar a análise de necessidades e a seleção de modelos de serviço (IaaS, PaaS, SaaS).
- Definir critérios para avaliação de fornecedores e requisitos de segurança.
- Alinhar a infraestrutura de TIC e a capacitação das equipes às novas tecnologias.
- Garantir a conformidade regulatória e a segurança jurídica.

A estratégia fundamenta-se em princípios como a preferência pelo modelo *cloud-first*, a mitigação de riscos de dependência tecnológica (*vendor lock-in*) e a promoção da portabilidade e interoperabilidade de dados. Articulada com os planos institucionais de tecnologia e segurança da informação, esta política visa consolidar uma governança robusta, garantindo a continuidade, a eficiência e a inovação dos serviços digitais que apoiam a missão de ensino, pesquisa e extensão da UFSCar.

2. Diretrizes Gerais

I. Análise e Autorização: Toda aquisição e uso de software corporativo deve ser previamente analisada e autorizada pela área de TI, garantindo aderência às necessidades institucionais e conformidade normativa. Recomenda-se a utilização de formulários padronizados e fluxos de aprovação eletrônicos, com registro de justificativas e pareceres técnicos.

II. Gestão de Dependência Tecnológica: Nos processos de contratação, avaliar e mitigar riscos de *vendor lock-in*, priorizando soluções com portabilidade e interoperabilidade. Recomenda-se incluir cláusulas contratuais que assegurem exportação de dados em formatos abertos e reversibilidade dos serviços.

III. Inventário de Softwares: Manter inventário atualizado de todos os softwares, com informações sobre licenças, contratos, datas de renovação, status de conformidade, responsáveis e registros de auditoria. Esta lista de inventário atualizado com as informações atualizadas deverá ser disponibilizada em página da rede, para ciência dos interessados.

2.1. Identificação das Necessidades do Negócio

I. Levantamento Detalhado: Realizar levantamento sistemático das necessidades institucionais, utilizando entrevistas, workshops e análise de processos. Documentar requisitos funcionais, de desempenho, segurança e compliance.

II. Planejamento de Migração: Detalhar o acesso aos recursos, níveis de serviço, integrações com sistemas legados e recursos computacionais e de armazenamento. Utilizar fluxogramas para documentar

o processo de decisão.

III. Viabilidade de Soluções em Nuvem: Avaliar sempre que possível a concepção de novas soluções “cloud-native”, aproveitando escalabilidade, flexibilidade e custo-benefício da nuvem.

2.2. Seleção dos Modelos Adequados

I. Compatibilidade Orçamentária: Escolher modelo (IaaS, PaaS, SaaS) compatível com restrições orçamentárias, buscando o melhor custo-benefício.

II. Criticidade das Informações: Natureza e criticidade dos dados orientam a escolha entre nuvem pública, privada, híbrida, comunitária ou de governo.

III. Plano de Recuperação: Para soluções totalmente em nuvem, prever plano de recuperação de serviços, incluindo backup, redundância e contingência, detalhando rotinas e responsabilidades.

2.3. Avaliação de Fornecedores

I. Participação Ampliada: Ampliar o rol de fornecedores aptos, promovendo concorrência e inovação.

II. Critérios de Seleção: Considerar experiência comprovada, aderência a normas de segurança, conformidade regulatória, disponibilidade, suporte técnico, escalabilidade e análise de custo total de propriedade.

III. Normativos Aplicáveis: Observar a Instrução Normativa GSI/PR nº 5/2021, Portaria SGD/MGI nº 5.950/2023 e demais normativos pertinentes.

2.4. Definição de Requisitos de Segurança

I. Classificação de Dados: Definir requisitos de segurança conforme sensibilidade dos dados, incluindo classificação, controles de acesso, criptografia em trânsito e repouso, autenticação multifator.

II. Avaliação de Controles: Avaliar controles de segurança dos fornecedores, auditorias externas, certificações (ISO 27001, SOC 2), conformidade nacional e internacional.

III. Gerenciamento de Riscos: Identificar sistemas e workloads migráveis sob a ótica da segurança, com medidas de mitigação para informações sigilosas.

2.5. Infraestrutura de TIC

I. Conectividade e Capacidade: Garantir infraestrutura adequada, com conexão estável, banda suficiente, redundância de links e ferramentas de monitoramento.

II. Avaliação Contínua: Avaliar periodicamente a infraestrutura, identificando necessidades de expansão, atualização e mitigação de pontos de falha. Recomenda-se uso de métricas de desempenho e planos de contingência.

2.6. Política de Governança

I. Papéis e Responsabilidades:

- **Ao Comitê de Governança Digital (CGD):** Compete aprovar e supervisionar a implementação desta Estratégia, definir diretrizes gerais e deliberar sobre casos omissos relacionados ao uso de software e serviços de computação em nuvem na UFSCar.

- **À Secretaria Geral de Informática (SIn):** Cabe planejar, contratar, gerenciar e operar os serviços de nuvem, zelar pela conformidade normativa e pela segurança da informação, manter o inventário de softwares e serviços em nuvem sempre atualizado e apoiar as unidades acadêmicas e administrativas na utilização adequada das soluções em nuvem.
- **Às unidades acadêmicas e administrativas da UFSCar:** É responsabilidade utilizar os serviços de nuvem de forma eficiente, segura e em conformidade com as diretrizes estabelecidas nesta Estratégia e nas orientações da SIn.

II. Gestão de Configuração:

A SIn deve assegurar a identificação e classificação de dados, o controle de acesso, o gerenciamento de configuração dos ambientes em nuvem e o monitoramento contínuo das atividades, garantindo que todas as operações estejam alinhadas às normas internas e externas de segurança e governança.

III. Supervisão Colegiada:

O Comitê de Governança Digital (CGD) supervisiona e aprova as decisões estratégicas relativas ao uso de computação em nuvem, além de estabelecer diretrizes gerais e deliberar sobre eventuais casos omissos, promovendo a integração entre as áreas de TI, as unidades acadêmicas e administrativas e a alta administração da UFSCar.

2.7. Princípios Norteadores

- I. **Cloud-First:** Priorizar soluções em nuvem, considerando custo, agilidade, escalabilidade e segurança.
- II. **Lift-and-Shift como Último Recurso:** Avaliar opções de otimização e modernização antes de migrar aplicações sem modificações.
- III. **Soluções Multicloud:** Adotar estratégias multicloud para evitar dependência de um único fornecedor, promovendo interoperabilidade e portabilidade.
- IV. **Segurança e Conformidade:** Implementar medidas robustas de segurança e garantir conformidade normativa.
- V. **Monitoramento e Governança Contínua:** Estabelecer mecanismos de monitoramento, auditoria e governança.
- VI. **Capacitação Contínua:** Oferecer treinamento e capacitação regular para equipes envolvidas.

3. Alinhamento com Planos Estratégicos

- I. **Integração e Sincronização:** Alinhar objetivos dos planos estratégicos (PDI e PDTIC) à estratégia global e à Política de Segurança da Informação da UFSCar.
- II. **Coerência e Consistência:** Garantir ações coerentes e evitar duplicidades.
- III. **Planejamento Participativo:** Envolver partes interessadas no planejamento, promovendo *feedback* contínuo e ajustes.
- IV. **Monitoramento e Avaliação:** Estabelecer mecanismos de monitoramento e avaliação periódica.
- V. **Flexibilidade e Adaptabilidade:** Manter planos flexíveis, com revisões periódicas para adaptação.

4. Metas e Benefícios

- I. **Linhas de Base:** Mapear o cenário atual (*AS IS*), identificando pontos fortes, fraquezas, oportunidades e ameaças.

II. **Metas Futuras:** Definir metas claras e mensuráveis para o estado desejado (*TO BE*), como agilidade, redução de custos, resiliência e segurança.

III. **Plano de Ação:** Desenvolver plano detalhado de transição, com etapas, recursos necessários e cronograma.

IV. **Monitoramento:** Implementar sistema de monitoramento contínuo para acompanhar progresso e realizar ajustes.

5. Capacitação

I. **Capacidades e Habilidades:** Desenvolver competências em infraestrutura de nuvem, segurança, projetos e análise de dados.

II. **Treinamento Contínuo:** Investir em treinamentos regulares e incentivar certificações reconhecidas.

III. **Especialização:** Promover especialização em áreas estratégicas, como segurança cibernética e desenvolvimento em nuvem.

IV. **Colaboração:** Fomentar comunicação e colaboração entre equipes.

6. Portabilidade e Interoperabilidade

I. **Portabilidade de Dados:** Garantir transferência de dados entre sistemas sem perda de integridade ou qualidade, utilizando formatos abertos.

II. **Interoperabilidade:** Adotar padrões abertos e tecnologias que permitam integração eficiente entre sistemas e serviços.

III. **Mitigação de Dependência:** Implementar medidas para reduzir dependência de fornecedores e evitar *vendor lock-in*.

IV. **Transparência e Segurança:** Assegurar processos transparentes e seguros para portabilidade e interoperabilidade.

7. Requisitos Regulatórios e Conformidade

I. **Cumprimento Legal:** Garantir conformidade com leis, regulamentos e normas internas, especialmente sobre proteção de dados pessoais.

II. **Documentação e Procedimentos:** Manter documentação adequada e seguir procedimentos estabelecidos.

III. **Auditorias e Inspeções:** Realizar auditorias e inspeções regulares.

IV. **Treinamento e Conscientização:** Implementar programas de treinamento e conscientização sobre conformidade e segurança.

8. Estratégia de Saída

I. **Análise de Dependências:** Avaliar dependências tecnológicas e operacionais entre sistemas e serviços.

II. **Portabilidade:** Planejar transferência de dados e serviços para outras plataformas.

III. **Backup e Redundância:** Implementar soluções de backup e redundância para garantir continuidade.

IV. **Contratos de Apoio:** Estabelecer contratos de apoio técnico e administrativo.

V. **Retorno à Infraestrutura Local:** Planejar retorno dos serviços à infraestrutura local, se necessário, para evitar *vendor lock-in*.

9. Análise de Riscos

- I. **Identificação de Riscos:** Reconhecer e documentar todos os riscos potenciais.
- II. **Avaliação e Mitigação:** Analisar probabilidade e impacto, implementando medidas de redução.
- III. **Monitoramento Contínuo:** Monitorar riscos e revisar medidas periodicamente, conforme a Portaria SGD/MGI nº 5.950/2023.

10. Uso Seguro de Computação em Nuvem

- I. **Requisitos Mínimos:** Observar requisitos mínimos de segurança da informação previstos em normas específicas.
- II. **Boas Práticas:** Implementar controles de segurança, monitoramento contínuo, auditorias e planos de resposta a incidentes.

11. Disposições Finais

- I. **Revisão e Atualização:** Esta Estratégia e seus documentos complementares devem ser revisados e atualizados periodicamente, conforme alterações legislativas, normativas e institucionais.
- II. **Divulgação:** As atualizações devem ser amplamente divulgadas a todos os usuários e partes interessadas.
- III. **Casos Omissos:** Os casos omissos serão tratados pelo Comitê de Governança Digital da UFSCar.



Documento assinado eletronicamente por **Erick Lazaro Melo, Secretário(a) Geral**, em 12/06/2025, às 16:39, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do [Decreto nº 8.539, de 8 de outubro de 2015](#).



A autenticidade deste documento pode ser conferida no site <https://sei.ufscar.br/autenticacao>, informando o código verificador **1884845** e o código CRC **D2914A61**.