



UNIVERSIDADE FEDERAL DE GOIÁS
DIRETORIA DE ADMINISTRAÇÃO DE PESSOAS

PORTARIA Nº 1086 DE 25 DE FEVEREIRO DE 2026

Dispõe sobre a Estratégia de Uso de Software e de Serviços de Computação em Nuvem no âmbito da Universidade Federal de Goiás.

A REITORA DA UNIVERSIDADE FEDERAL DE GOIÁS, no uso das atribuições definidas pelo art. 56 do Regimento Geral, e tendo em vista:

As atribuições definidas ao COMITÊ DE TECNOLOGIA DA INFORMAÇÃO pela Resolução CONSUNI nº 18/2018;

CONSIDERANDO a Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);

CONSIDERANDO a Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

CONSIDERANDO o Decreto nº 10.046, de 9 de outubro de 2019, que dispõe sobre a governança no compartilhamento de dados no âmbito da administração pública federal;

CONSIDERANDO a Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 (Processo de Contratação de Soluções de TIC);

CONSIDERANDO a Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 (Modelo de Contratação de Software e Serviços em Nuvem);

CONSIDERANDO a Portaria SGD/MGI nº 852, de 28 de março de 2023 (Programa de Privacidade e Segurança da Informação).

CONSIDERANDO as normas ISO/IEC 20000-1:2018, ISO/IEC 27001:2022, ISO/IEC 27002:2022 e ISO/IEC 27005:2022;

CONSIDERANDO os princípios e boas práticas do framework COBIT 2019;

RESOLVE:

Art. 1º Aprovar a Estratégia de Uso de Software e Serviços de Computação em Nuvem da Universidade Federal de Goiás.

ANEXO DA PORTARIA Nº 01/2025 CTI**ESTRATÉGIA DE USO DE SOFTWARE E SERVIÇOS DE COMPUTAÇÃO EM NUVEM DA UFG****CAPÍTULO I****DO ESCOPO**

1. **Art. 1º** A Estratégia de Uso de Software e de Serviços de Computação em Nuvem tem por objetivo assegurar que a Universidade Federal de Goiás obtenha resultados esperados com eficiência, economicidade, segurança e transparência, mitigando riscos associados à adoção e operação de tecnologias e modalidades de contratação de soluções de tecnologia da informação e comunicação.

2. **Art. 2º** Esta Estratégia aplica-se a novas contratações e às operações em curso de software e de serviços de computação em nuvem, compreendendo, entre outros:

- I - software sob o modelo de licenciamento permanente de direitos de uso;
- II - **software sob o modelo de cessão temporária ou por subscrição (SaaS - Software as a Service);**
- III - **infraestrutura como serviço (IaaS - Infrastructure as a Service);**
- IV - **plataforma como serviço (PaaS - Platform as a Service);**
- V - **suporte técnico e operação de recursos em nuvem;**
- VI - **migração, integração e monitoramento de serviços de computação em nuvem;**
- VII - **consultoria especializada em software e/ou serviços de computação em nuvem;**
- VIII - **soluções híbridas ou multinuvem implantadas pela UFG ou por terceiros sob contrato; e**
- IX - **práticas de gestão de custos e desempenho (FinOps - *Financial Operations*).**

CAPÍTULO II**DOS CONCEITOS E DEFINIÇÕES**

3. **Art. 3º** Para os fins desta estratégia, adotam-se os seguintes conceitos e definições:

- I - **Computação em nuvem:** modelo de provisão sob demanda de recursos e serviços computacionais acessíveis por rede, com elasticidade e autoatendimento;
- II - **Modelos de implantação de nuvem:** pública, privada, híbrida e comunitária, incluindo nuvem de governo;
- III - **IaaS, PaaS e SaaS:** modelos de serviço em nuvem para infraestrutura, plataforma e software, respectivamente;
- IV - **Carga de trabalho (workload):** conjunto de componentes técnicos que suportam serviços de TIC e requisitos de negócio;

- V - **Lift and Shift:** estratégia de migração que re-hospeda aplicativos e dados “como estão” do data center para a nuvem (IaaS), com mínimas ou nenhuma mudança no código.
- VI - **Instância de computação:** máquina virtual e serviços associados para operação em nuvem;
- VII - **Banco de dados como serviço (DBaaS - Database as a Service) e função como serviço (FaaS - Function as a Service):** serviços gerenciados de dados e de execução de funções sob demanda;
- VIII - **Multinuvem (Multicloud):** uso coordenado de recursos de dois ou mais provedores de nuvem;
- IX - **Integrador de serviços em nuvem (cloud broker):** agente que integra, gerencia e otimiza o uso de múltiplos provedores de nuvem;
- X - **Plataforma de gerenciamento de nuvem (CMP - Cloud Management Platform):** sistema para provisionamento, monitoramento, segurança, custos, identidade e automação em múltiplos provedores;
- XI - **Disponibilidade:** condição de serviço ou recurso estar acessível e apto a cumprir suas funções dentro do período acordado;
- XII - **Incidente e incidente de segurança da informação:** eventos que reduzam a qualidade ou ameacem a segurança de serviços e informações;
- XIII - **Tratamento da informação:** ações de produção, uso, armazenamento, transmissão, descarte e controle de informações;
- XIV - **Suporte técnico:** atendimento e orientação para solução de problemas relativos ao serviço contratado.

CAPÍTULO III

DOS PRINCÍPIOS

4. **Art. 4º** A adoção de *software* e de serviços de computação em nuvem no âmbito da UFG observará os seguintes princípios:

- I - legalidade, impessoalidade, moralidade, publicidade e eficiência;
- II - integridade, autenticidade, disponibilidade e confidencialidade da informação, com observância à transparência e às restrições legais aplicáveis;
- III - alinhamento com o planejamento institucional, o Plano Diretor de TIC e a Política de Governança Digital;
- IV - responsabilidade e prestação de contas (*accountability*), com segregação de funções e papéis definidos conforme modelo RACI;
- V - conformidade com a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018) e com as normas ISO/IEC 27001, 27002, 27005 e 20000-1;
- VI - gestão de riscos contínua, preventiva e integrada aos processos de governança e segurança da informação;

- VII - capacitação e conscientização permanentes dos usuários e gestores sobre boas práticas de segurança e governança;
- VIII - adoção do princípio *cloud first*, precedido de análise técnica, regulatória, orçamentária e de segurança;
- IX - uso de estratégias *lift and shift* apenas quando tecnicamente justificadas e após avaliação de desempenho e custo-benefício;
- X - incentivo ao uso de soluções híbridas e multinuvem que promovam resiliência, interoperabilidade e redução de dependência tecnológica.

CAPÍTULO IV

DAS DISPOSIÇÕES GERAIS

5. **Art. 5º** A comprovação de conformidade em segurança da informação poderá incluir relatórios de auditorias e certificações reconhecidas, conforme exigências definidas em cada contratação, sem prejuízo de verificações adicionais pela UFG.

5.1. **Parágrafo único:** Quando houver *cloud broker*, caberá a ele apresentar evidências de conformidade de todos os provedores que representar e garantir a aderência aos requisitos contratuais e de segurança da UFG.

CAPÍTULO V

DAS DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO

1. SEÇÃO I: DA IDENTIFICAÇÃO DAS NECESSIDADES DO NEGÓCIO

6. **Art. 6º** Antes da contratação, a UFG identificará e avaliará as necessidades de negócio, definindo:

- I - sistemas, aplicações, dados e serviços elegíveis à nuvem;
- II - perfil de acesso, níveis de serviço e requisitos de desempenho;
- III - recursos e capacidades computacionais previstos.

2. SEÇÃO II: DA SELEÇÃO DOS MODELOS ADEQUADOS

7. **Art. 7º** A UFG avaliará modelos de serviço e de implantação, considerando:

- I - maturidade técnica e regulatória das unidades demandantes;
- II - aderência a requisitos de segurança, privacidade e continuidade;
- III - economicidade e custo total de propriedade;
- IV - interoperabilidade, portabilidade e mitigação de *lock-in*.

7.1. **§1º** Na ausência de maturidade técnica suficiente ou diante de impedimentos regulatórios, recomenda-se abordagem de nuvem híbrida.

7.2. **§2º** Quando comprovada a viabilidade integral em nuvem, poderá ser adotada abordagem totalmente em nuvem, inclusive prevendo migrações do ambiente local.

3. **SEÇÃO III: DA AVALIAÇÃO DE FORNECEDORES**

8. **Art. 8º** Os estudos técnicos preliminares considerarão, entre outros:

- I - segurança da informação e privacidade;
- II - conformidade com requisitos legais e institucionais;
- III - disponibilidade, desempenho e suporte;
- IV - capacidade técnica, certificações e experiência comprovada.

4. **SEÇÃO IV: DA DEFINIÇÃO DE REQUISITOS DE SEGURANÇA**

9. **Art. 9º** A UFG estabelecerá requisitos de segurança mandatórios e complementares, incluindo:

- I - classificação e tratamento de dados por criticidade e sigilo;
- II - políticas de controle de acesso e identidade;
- III - proteção criptográfica conforme criticidade;
- IV - monitoramento, registro e auditoria independentes;
- V - resposta a incidentes e continuidade de negócios.

5. **SEÇÃO V: DA GOVERNANÇA E MONITORAMENTO**

10. **Art. 10** A governança abrangerá:

- I - identificação e classificação de ativos e dados;
- II - papéis e responsabilidades claras para áreas de TIC, negócio e nuvem;
- III - gestão de configuração, mudanças e vulnerabilidades;
- IV - medição de níveis de serviço com penalidades por não conformidade; e
- V - supervisão pelo Comitê de Tecnologia da Informação da UFG, quando aplicável.

10.1. **Parágrafo único.** A governança prevista neste artigo observará a Política de Governança de Dados da Administração Pública Federal, nos termos do Decreto nº 10.046/2019 e atos supervenientes, especialmente quanto a papéis, responsabilidades, compartilhamento e qualidade de dados.

6. **SEÇÃO VI: DO USO SEGURO DE SOFTWARE E DE SERVIÇOS EM NUVEM**

11. **Art. 11** A UFG definirá políticas e normas internas para uso seguro, contemplando:

- I - elegibilidade de cargas de trabalho;
- II - requisitos mínimos de segurança por tipo de serviço;
- III - medidas de gerenciamento de risco;
- IV - diretrizes para ambientes de desenvolvimento, teste e produção;
- V - requisitos para uso de marketplace, quando aplicável.

7. **SEÇÃO VII: DA INFRAESTRUTURA DE TIC DE SUPORTE**

12. **Art. 12** A UFG assegurará:

- I - conectividade estável e capacidade de banda compatível;
- II - mecanismos de redundância e contingência;
- III - ferramentas de monitoramento, observabilidade e gestão de custos.

8. **SEÇÃO VIII: DA GOVERNANÇA DA NUVEM**

13. **Art. 13** A UFG definirá papéis e responsabilidades, incluindo:

- I - gestor do contrato;
- II - fiscal técnico;
- III - responsáveis por segurança da informação e proteção de dados;
- IV - pontos focais das unidades demandantes.

9. **SEÇÃO IX: DO ALINHAMENTO COM OUTROS PLANOS**

14. **Art. 14** A estratégia alinhar-se-á, no que couber, a:

- I - Plano de Desenvolvimento Institucional (PDI);
- II - Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC);
- III - Plano de Contratações Anual (PCA).

10. **SEÇÃO X: DAS LINHAS DE BASE E METAS**

15. **Art. 15** A UFG estabelecerá linhas de base e metas relacionadas a:

- I - agilidade e tempo de entrega;
- II - custo total de propriedade e otimização de consumo;
- III - resiliência e continuidade;
- IV - segurança e conformidade.

11. **SEÇÃO XI: DA CAPACITAÇÃO**

16. **Art. 16** A UFG promoverá capacitação continuada para equipes que gerenciem, operem ou utilizem recursos em nuvem, considerando:

- I - competências técnicas específicas por provedor;
- II - segurança, privacidade e conformidade;
- III - práticas de *finops*, *devops* e *secops*.

12. **SEÇÃO XII: DA PORTABILIDADE E INTEROPERABILIDADE**

17. **Art. 17** A UFG adotará medidas para mitigar dependência tecnológica, considerando:

- I - padrões abertos e interoperáveis;

- II - containerização e orquestração;
- III - alternativas de banco de dados e serviços gerenciados;
- IV - estratégias multinuvem e/ou híbridas.

13. **SEÇÃO XIII: DOS REQUISITOS REGULATÓRIOS E DE CONFORMIDADE**

18. **Art. 18** A UFG observará requisitos regulatórios, de proteção de dados e de segurança da informação aplicáveis às atividades acadêmicas, administrativas e de pesquisa, inclusive quanto à custódia, circulação e guarda de informações sensíveis, bem como as disposições do Decreto nº 10.046/2019, no que couber

18.1. **§1º** Para fins desta Estratégia, distinguem-se:

- I - informação classificada, nos termos da Lei nº 12.527/2011 (LAI), com fundamento em interesse público e segurança institucional;
- II - dado pessoal sensível, nos termos do art. 5º, II, e art. 11 da Lei nº 13.709/2018 (LGPD);
- III - dado tratado para fins de pesquisa científica, histórica ou estatística, observado o regime jurídico específico dos arts. 7º, §4º, e 13 da LGPD.

18.2. **§2º** O tratamento em nuvem de dados pessoais sensíveis ou de dados utilizados para fins de pesquisa observará medidas reforçadas de segurança, sigilo e rastreabilidade, compatíveis com sua natureza e base legal de tratamento.

14. **SEÇÃO XIV: DA ESTRATÉGIA DE SAÍDA**

19. **Art. 19** A UFG definirá diretrizes de saída, contemplando:

- I - portabilidade de dados e aplicações;
- II - prazos e formatos de entrega;
- III - devolução e descarte seguro;
- IV - continuidade operacional durante a transição.

15. **SEÇÃO XV: DA ANÁLISE DE RISCOS**

20. **Art. 20** A UFG manterá processo de gerenciamento de riscos para adoção e operação em nuvem, incluindo:

- I - identificação e avaliação de riscos;
- II - plano de tratamento;
- III - monitoramento contínuo;
- IV - reporte à alta administração, quando aplicável.

CAPÍTULO VI

DOS REQUISITOS PARA USO SEGURO EM NUVEM

21. **Art. 21** Os requisitos técnicos detalhados para uso seguro em nuvem serão disciplinados em norma específica da UFG/CTI, observando, no que couber, as disposições e diretrizes vigentes da Administração Pública Federal.

CAPÍTULO VII

DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES

16. **SEÇÃO I: DA ALTA ADMINISTRAÇÃO**

22. **Art. 22** Compete à alta administração:

- I - assegurar a implementação desta estratégia;
- II - prover recursos financeiros, tecnológicos e humanos necessários.

17. **SEÇÃO II: DO COMITÊ DE TECNOLOGIA DA INFORMAÇÃO DA UFG**

23. **Art. 23** Compete ao Comitê de Tecnologia da Informação da UFG:

- I - aprovar minutas de elaboração e revisão desta estratégia e de normas correlatas de uso seguro em nuvem;
- II - definir, quando necessário, diretrizes adicionais sobre localização de dados e requisitos criptográficos mínimos;
- III - decidir, em caráter conclusivo, sobre propostas de atualização desta estratégia;
- IV - supervisionar contratos de alta materialidade ou relevância estratégica, quando aplicável.

18. **SEÇÃO III: DO PRESIDENTE DO COMITÊ DE SEGURANÇA DA INFORMAÇÃO**

24. **Art. 24** Compete ao presidente do comitê de segurança da informação:

- I - coordenar a elaboração e revisão de normas sobre estratégia e uso seguro em nuvem;
- II - supervisionar a aplicação das normas internas;
- III - assegurar comunicação e verificação de controles e níveis de serviço de segurança junto a provedores;
- IV - supervisionar correções e tratativas de desvios;
- V - comunicar incidentes cibernéticos às instâncias competentes;
- VI - submeter minutas à alta administração;
- VII - propor ações de melhoria contínua em segurança.

19. **SEÇÃO IV: DA SECRETARIA DE TECNOLOGIA E INFORMAÇÃO E SETORES DE OPERAÇÕES LOCAIS DE TIC**

25. **Art. 25** Compete à Secretaria de Tecnologia e Informação e os Setores de Operações Locais de TIC:

- I - implementar procedimentos relativos ao uso de nuvem conforme esta estratégia e normas correlatas;

- II - manter inventário, observabilidade, trilhas de auditoria e relatórios de desempenho;
- III - executar controles de custos, orçamento e otimização de consumo;
- IV - apoiar as unidades demandantes na elaboração de estudos e termos de referência.

CAPÍTULO VIII

DAS DIRETRIZES AMPLAS PARA TRATAMENTO DE INFORMAÇÃO CLASSIFICADA EM NUVEM

26. **Art. 26** No que couber e quando aplicável à UFG, o tratamento de informação classificada observará diretrizes amplas para ambientes de nuvem, incluindo:

- I - uso de nuvem privada ou comunitária gerida por órgãos públicos ou empresas públicas, com isolamento lógico e físico adequado;
- II - segmentação de rede para isolar ambientes de processamento e armazenamento;
- III - tecnologias de virtualização e, quando aplicável, de contêineres com controles de isolamento e segurança específicos;
- IV - criptografia de dados em repouso e em trânsito, com gestão de chaves sob controle da instituição;
- V - processos de backup e recuperação com cópias criptografadas mantidas em infraestrutura sob controle institucional;
- VI - autenticação multifatorial para acessos a ambientes que tratem informação classificada; políticas de necessidade de conhecer e credenciamento de pessoal;
- VII - registro detalhado e imutável de acessos e operações, com auditorias periódicas independentes;
- VIII - alertas automatizados para atividades suspeitas;
- IX - gestão centralizada de identidades, permissões e revogação com trilhas completas de auditoria;
- X - modelos de controle de acesso por papéis e por atributos, com revisões periódicas;
- XI - medidas técnicas e administrativas que impeçam o acesso do provedor ao conteúdo das informações.

27. **Art. 27** Quando cabível, a circulação e o armazenamento de informações classificadas observarão, de forma ampla:

- I - processamento e guarda em centros de dados em território nacional;
- II - restrições ao trânsito internacional, admitidas exceções institucionais justificadas e com proteção criptográfica compatível;
- III - mecanismos de rastreabilidade, registro e monitoração integral de tráfego;
- IV - previsão contratual de acesso irrestrito a registros e evidências pela equipe de segurança da instituição.

27.1. **Parágrafo único.** A adoção destas diretrizes será avaliada caso a caso pela UFG, nos limites de sua competência, natureza da informação tratada e legislações aplicáveis.

CAPÍTULO IX

DAS DIRETRIZES AMPLAS PARA PROVEDORES E BROKERS

28. **Art. 28** Os provedores de serviço de nuvem e cloud brokers deverão, no que couber:
- I - demonstrar capacidade técnica, conformidade e certificações pertinentes;
 - II - disponibilizar infraestrutura e controles compatíveis com exigências de segurança, continuidade e localização de dados definidas pela UFG;
 - III - assegurar trilhas de auditoria, relatórios periódicos e cooperação em investigações;
 - IV - viabilizar credenciamento e controles de acesso de pessoal;
 - V - atender a inspeções e auditorias técnicas previstas em contrato.

CAPÍTULO X**DA REVISÃO E ATUALIZAÇÃO**

29. **Art. 29** Esta estratégia e seus documentos decorrentes serão revisados e atualizados:
- I - diante de alterações legais, regulatórias ou institucionais;
 - II - por diretrizes do Comitê de Tecnologia da Informação da UFG;
 - III - a cada até 2 (dois) anos, ou antes, em razão de novos requisitos tecnológicos, de segurança ou de continuidade;
 - IV - após eventos relevantes de segurança da informação.

CAPÍTULO XI**DAS DISPOSIÇÕES FINAIS**

30. **Art. 30** As novas contratações de software e serviços em nuvem observarão esta estratégia e os modelos e diretrizes de contratação vigentes no âmbito da Administração Pública Federal, no que couber.
31. **Art. 31** Esta estratégia será divulgada a usuários e partes interessadas para promover sua observância.
32. **Art. 32** A alta administração proverá os recursos necessários à execução desta estratégia.
33. **Art. 33** Os casos omissos serão analisados pelo Comitê de Tecnologia da Informação da UFG.
34. **Art. 34** Esta norma entra em vigor na data de sua publicação.

ANEXO TÉCNICO – DIRETRIZES DE GOVERNANÇA, SEGURANÇA E GESTÃO DE RISCOS EM NUVEM

20. **1. MATRIZ DE CONTROLES DE SEGURANÇA DA INFORMAÇÃO (ISO/IEC 27001:2022 E 27002:2022)**

Controle ISO 27001 / 27002	Descrição do Controle	Aplicabilidade à UFG
5.1 Políticas de Segurança da Informação	Políticas aprovadas, comunicadas e revisadas periodicamente.	Aplicável a todas as unidades da UFG.
5.2 Papéis e Responsabilidades	Definição clara de responsabilidades conforme modelo RACI.	Aplicável.

Controle ISO 27001 / 27002	Descrição do Controle	Aplicabilidade à UFG
5.7 Inteligência de Ameaças	Monitoramento contínuo de ameaças e vulnerabilidades.	Aplicável à STI e CGD.
5.15 Inventário de Ativos	Inventário atualizado de recursos e dados em nuvem.	Aplicável à STI.
6.3 Controles de Acesso	Gestão de identidade, autenticação multifatorial e segregação de funções.	Obrigatório.
8.4 Backup e Recuperação	Política de backup 3-2-1 e testes de restauração semestrais.	Aplicável.
8.9 Gestão de Vulnerabilidades	Correção de falhas críticas em até 15 dias.	Aplicável à STI e provedores.
8.13 Registro e Auditoria	Logs imutáveis, retidos por 12 meses, com revisão trimestral.	Aplicável a todos os serviços críticos.

21. 2. MATRIZ DE RISCOS E TRATAMENTO (ISO/IEC 27005:2022)

Risco Identificado	Probabilidade	Impacto	Nível de Risco	Plano de Tratamento
Falha de autenticação em serviço em nuvem	Alta	Alta	Crítico	Implementar MFA e revisão trimestral de acessos.
Perda de dados sensíveis por falha de backup	Média	Alta	Alto	Política 3-2-1 e testes semestrais de restauração.
Dependência de único provedor (lock-in)	Alta	Média	Alto	Estratégia multinuvem e cláusulas contratuais de portabilidade.
Incidente de vazamento de dados	Baixa	Crítico	Crítico	Criptografia ponta a ponta e plano de resposta a incidentes.
Falta de capacitação das equipes	Média	Média	Moderado	Capacitação contínua em FinOps, DevSecOps e LGPD.

22. 3. DIRETRIZES DE AUDITORIA E CONFORMIDADE

As auditorias deverão avaliar, no mínimo:

- Conformidade com ISO/IEC 20000-1, 27001, 27002 e 27005;
- Evidências documentais de controle de acesso, backup e gestão de vulnerabilidades;
- Tratamento de riscos e eficácia dos planos de ação;
- Adoção de políticas de melhoria contínua e cultura de segurança.

SANDRAMARA MATIAS CHAVES



Documento assinado eletronicamente por **Sandramara Matias Chaves, Reitora**, em 25/02/2026, às 14:48, conforme horário oficial de Brasília, com fundamento no § 3º do art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).



A autenticidade deste documento pode ser conferida no site https://sei.ufg.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **6005017** e o código CRC **E217BDD4**.

