



Ministério da Educação  
Universidade Federal do Cariri  
Comitê de Governança

ATO DECISÓRIO CG N.º 15, DE 07 DE OUTUBRO DE 2025

Aprova a Estratégia de uso de Software e de Serviços de Computação em Nuvem da UFCA.

O **PRESIDENTE DO COMITÊ DE GOVERNANÇA DA UNIVERSIDADE FEDERAL DO CARIRI - UFCA**, no uso da competência que lhe confere o Decreto Presidencial de 1º de junho de 2023, publicado no Diário Oficial da União, no dia 02 de junho de 2023, seção 2, página 1, e tendo em vista o que deliberou o Comitê de Governança - CG em sua Reunião Ordinária, em 07 de outubro de 2025, na forma do que dispõe o art. 8 do Regimento Interno do Comitê de Governança, resolve:

Art. 1º Aprovar a Estratégia de uso de Software e de Serviços de Computação em Nuvem da Universidade Federal do Cariri, nos termos do Anexo 1 deste Ato Decisório: [Documento PDF] [Estratégia de uso de Software e de Serviços de Computação em Nuvem](#).

Art. 2º Este Ato Decisório entra em vigor nesta data.



*Documento assinado digitalmente*  
SILVÉRIO DE PAIVA FREITAS JÚNIOR  
Presidente do Comitê de Governança



Ministério da Educação  
Universidade Federal do Cariri  
Comitê de Governança

## ANEXOS

- ANEXO 01 - DOCUMENTO: [Estratégia de uso de Software e de Serviços de Computação em Nuvem.](#)



**MINISTÉRIO DA EDUCAÇÃO  
UNIVERSIDADE FEDERAL DO CARIRI  
DIRETORIA DE TECNOLOGIA DA INFORMAÇÃO**

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

Dispõe sobre a estratégia de uso de software e de serviços de computação em nuvem no âmbito da Universidade Federal do Cariri (UFCA).

**CAPÍTULO I  
DO ESCOPO**

Art. 1º A estratégia de uso de software e de serviços de computação em nuvem tem por objetivo assegurar que a UFCA obtenha resultados esperados, com eficiência, economicidade e segurança, e mitigue riscos associados à adoção de tecnologias e modalidades de contratação de soluções de tecnologia da informação e comunicação.

Art. 2º Esta estratégia aplica-se a novas contratações de software e de serviços de computação em nuvem no âmbito da UFCA, compreendendo:

- 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 por subscrição ou como serviço (SaaS);
- IV - infraestrutura como serviço (IaaS);
- V - plataforma como serviço (PaaS);
- VI - suporte técnico relacionado;
- VII - operação e gerenciamento de recursos em nuvem;
- VIII - migração de recursos para ambiente de nuvem;
- IX - integração de serviços de computação em nuvem; e
- X - consultoria especializada em software e/ou serviços de computação em nuvem.

**CAPÍTULO II  
DAS REFERÊNCIAS**

Art. 3º A implementação desta estratégia observará, no que couber, as seguintes normas e atos:

- I - Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação);
- II - Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);
- III - Lei nº 14.133, de 1º de abril de 2021 (Lei de Licitações e Contratos Administrativos);
- IV - Decreto nº 7.845, de 14 de novembro de 2012 (segurança de informações classificadas);
- V - Decreto nº 9.637, de 26 de dezembro de 2018 (Política Nacional de Segurança da Informação), com alterações do Decreto nº 10.641, de 2 de março de 2021;

- VI - Decreto nº 10.222, de 5 de fevereiro de 2020 (Estratégia Nacional de Segurança Cibernética – E-Ciber);
- VII - Decreto nº 12.572, de 4 de agosto de 2025 (disposições correlatas citadas em normativos de segurança);
- VIII - Instrução Normativa GSI/PR nº 5, de 30 de agosto de 2021 (requisitos mínimos de segurança da informação para uso de nuvem na APF);
- IX - Instrução Normativa GSI/PR nº 8, de 6 de outubro de 2025 (requisitos para tratamento de informação classificada em nuvem);
- X - Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022 (processo de contratação de soluções de TIC);
- XI - Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023 (modelo de contratação de software e serviços em nuvem);
- XII - Portaria SGD/MGI nº 852, de 28 de março de 2023 (Programa de Privacidade e Segurança da Informação);
- XIII - Normas técnicas ABNT NBR ISO/IEC 27001, 27017, 27018, 27701 e 22237 (boas práticas de segurança da informação e de data centers).

### **CAPÍTULO III DOS CONCEITOS E DEFINIÇÕES**

Art. 4º Para 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 - instância de computação: máquina virtual e serviços associados para operação em nuvem;
- VI - banco de dados como serviço (DBaaS) e função como serviço (FaaS): serviços gerenciados de dados e de execução de funções sob demanda;
- VII - multinuvm (multicloud): uso coordenado de recursos de dois ou mais provedores de nuvem;
- VIII - integrador de serviços em nuvem (cloud broker): agente que integra, gerencia e otimiza o uso de múltiplos provedores de nuvem;
- IX - plataforma de gerenciamento de nuvem (CMP): sistema para provisionamento, monitoramento, segurança, custos, identidade e automação em múltiplos provedores;
- X - catálogo de serviços de computação em nuvem: lista padronizada de serviços de nuvem adotada pela UFCA para identificação, mensuração e contratação;
- 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 IV DOS PRINCÍPIOS**

Art. 5º A adoção de software e serviços de computação em nuvem observará os seguintes princípios:

- I - legalidade, impessoalidade, moralidade, publicidade e eficiência;
- II - integridade, autenticidade, disponibilidade e confidencialidade da informação, com transparência e restrições nos termos legais;
- III - alinhamento com planejamento institucional e governança de TIC;
- IV - responsabilidade pelas normas de segurança da informação;
- V - educação, conscientização e comunicação contínuas em segurança;
- VI - cloud first, com avaliação técnica e de riscos;
- VII - lift and shift como último recurso;
- VIII - broker multinuvel para reduzir dependência e otimizar custo, desempenho e resiliência.

## **CAPÍTULO V DAS DISPOSIÇÕES GERAIS**

Art. 6º 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 UFCA.

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 UFCA.

## **CAPÍTULO VI DAS DIRETRIZES PARA DEFINIÇÃO DA ESTRATÉGIA DE USO**

### **Seção I**

#### **Da identificação das necessidades do negócio**

Art. 7º Antes da contratação, a UFCA 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.

### **Seção II**

#### **Da seleção dos modelos adequados**

Art. 8º A UFCA 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.

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

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

### **Seção III**

#### **Da avaliação de fornecedores**

Art. 9º 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.

### **Seção IV**

#### **Da definição de requisitos de segurança**

Art. 10. A UFCA 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.

### **Seção V**

#### **Da governança e do monitoramento**

Art. 11. 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;
- V - supervisão pelo Comitê de Governança da UFCA, quando aplicável.

### **Seção VI**

#### **Do uso seguro de software e de serviços em nuvem**

Art. 12. A UFCA 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.

## **Seção VII**

### **Da infraestrutura de TIC de suporte**

Art. 13. A UFCA assegurará:

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

## **Seção VIII**

### **Da governança da nuvem**

Art. 14. A UFCA 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.

## **Seção IX**

### **Do alinhamento com outros planos**

Art. 15. A estratégia alinhar-se-á, no que couber, a:

- I - Plano de Desenvolvimento Institucional;
- II - Plano Diretor de Tecnologia da Informação;
- III - Plano de Contratações Anual;
- IV - Plano de Gestão de Segurança da Informação (quando aplicável).

## **Seção X**

### **Das linhas de base e metas**

Art. 16. A UFCA 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.

## **Seção XI**

### **Da capacitação**

Art. 17. A UFCA 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.

## **Seção XII**

### **Da portabilidade e interoperabilidade**

Art. 18. A UFCA 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.

## **Seção XIII**

### **Dos requisitos regulatórios e de conformidade**

Art. 19. A UFCA 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.

## **Seção XIV**

### **Da estratégia de saída**

Art. 20. A UFCA 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.

## **Seção XV**

### **Da análise de riscos**

Art. 21. A UFCA 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 VII DOS REQUISITOS PARA USO SEGURO EM NUVEM**

Art. 22. Os requisitos técnicos detalhados para uso seguro em nuvem serão disciplinados em norma específica da UFCA, observando, no que couber, as disposições e diretrizes vigentes da Administração Pública Federal.

## **CAPÍTULO VIII DAS COMPETÊNCIAS, ATRIBUIÇÕES E RESPONSABILIDADES**

### **Seção I Da alta administração**

Art. 23. Compete à alta administração:

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

### **Seção II Do Comitê de Governança da UFCA**

Art. 24. Compete ao Comitê de Governança da UFCA:

- 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.

### **Seção III Do gestor de segurança da informação**

Art. 25. Compete ao gestor 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.

### **Seção IV Da Diretoria de Tecnologia da Informação e unidades de TIC**

Art. 26. Compete à Diretoria de Tecnologia da Informação e às unidades e servidores 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 IX**

### **DAS DIRETRIZES AMPLAS PARA TRATAMENTO DE INFORMAÇÃO CLASSIFICADA EM NUVEM**

Art. 27. No que couber e quando aplicável à UFCA, 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;
- VII - políticas de necessidade de conhecer e credenciamento de pessoal;
- VIII - registro detalhado e imutável de acessos e operações, com auditorias periódicas independentes;
- IX - alertas automatizados para atividades suspeitas;
- X - gestão centralizada de identidades, permissões e revogação com trilhas completas de auditoria;
- XI - modelos de controle de acesso por papéis e por atributos, com revisões periódicas;
- XII - medidas técnicas e administrativas que impeçam acesso do provedor ao conteúdo das informações.

Art. 28. 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.

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

## **CAPÍTULO X DAS DIRETRIZES AMPLAS PARA PROVEDORES E BROKERS**

Art. 29. 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 UFCA;
- 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 XI DA REVISÃO E ATUALIZAÇÃO**

Art. 30. Esta estratégia e seus documentos decorrentes serão revisados e atualizados:

- I - diante de alterações legais, regulatórias ou institucionais;
- II - por diretrizes do Comitê de Governança da UFCA;
- 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 XII DAS DISPOSIÇÕES FINAIS**

Art. 31. 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.

Art. 32. Esta estratégia será divulgada a usuários e partes interessadas para promover sua observância.

Art. 33. A alta administração proverá os recursos necessários à execução desta estratégia.

Art. 34. Os casos omissos serão analisados pelo Comitê de Governança da UFCA.

Art. 35. Esta norma entra em vigor na data de sua publicação.