

UNIVERSIDADE FEDERAL DO TOCANTINS
CONSELHO UNIVERSITÁRIO - CONSUNI

Secretaria dos Conselhos Superiores (Socs)
Bloco IV, Segundo Andar, Câmpus de Palmas
(63) 3229-4067 | (63) 3229-4238 | socs@uft.edu.br



RESOLUÇÃO Nº 101, DE 08 DE NOVEMBRO DE 2023 – CONSUNI/UFT

Estabelece a Política de Computação em Nuvem com as diretrizes de orientação, monitoramento e avaliação no âmbito da Universidade Federal do Tocantins (UFT).

O Egrégio Conselho Universitário (Consuni) da Universidade Federal do Tocantins (UFT), reunido em sessão ordinária realizada no dia 08 de novembro de 2023, no uso de suas atribuições legais e estatutárias, e

CONSIDERANDO, que os riscos decorrentes de falhas na gestão da segurança da informação são de toda ordem e podem representar desde problemas relacionados à integridade de dados públicos e pessoais, passando pelo vazamento de informações sigilosas, confidenciais e pessoais, bem como, podendo provocar impactos econômicos negativos em caso de indisponibilidade de serviços ou falhas em sistemas e bases de dados;

CONSIDERANDO, a Instrução Normativa nº 05/GSI/PR, de 30 de agosto de 2021, que trata do requisito mínimo de segurança da informação para utilização de soluções de computação em nuvem pelos órgãos e pelas entidades da administração pública federal;

CONSIDERANDO, o Capítulo IV da Instrução Normativa nº 03/GSI/PR, de 28 de maio de 2021, que trata da Gestão da Continuidade de Negócios em Segurança da Informação;

CONSIDERANDO, o Decreto nº 10.332/2020, que institui a Estratégia de Governo Digital 2020-2022;

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

CONSIDERANDO, a Lei nº 13.709/2018, de 14 de agosto de 2018, que institui a Lei Geral de Proteção de Dados (LGPD) que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;

CONSIDERANDO, o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação (PNSI), dispõe sobre a governança da segurança da informação, no âmbito da administração pública federal, com a finalidade de assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional;

CONSIDERANDO, os incisos I, II e III do Decreto nº 9.573/2018, que aprovou a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC);

CONSIDERANDO, os itens 2.3.4. e 2.3.5. do Decreto nº 10.222/2020 - Estratégia Nacional de Segurança Cibernética (E-CIBER) que tratam da elevação dos níveis de proteção das infraestruturas críticas;

CONSIDERANDO, o inciso XXIII, Art. 2º do Decreto nº 10.046/2019, que trata da Governança no Compartilhamento de Dados (GCD), em especial, das ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

CONSIDERANDO, o item 12.3 da Norma ABNT NBR ISO/IEC 27001:2013 Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação - Requisitos, que trata sobre Cópia de Segurança;

CONSIDERANDO, o Decreto nº 9.637/2018 que aprova a Política Nacional de Segurança da Informação - PNSI que abrange segurança cibernética, defesa cibernética, segurança física e a proteção de dados organizacionais,

RESOLVE:

Art. 1º Aprovar a Política de Computação em Nuvem da Universidade Federal do Tocantins (UFT), conforme anexo desta Resolução.

Art. 2º A Política de Computação em Nuvem da Universidade Federal do Tocantins observará os princípios, objetivos e diretrizes estabelecidos nesta Política, bem como às disposições constitucionais, legais e regimentais vigentes.

Art. 3º As determinações desta política aplicam-se a novas contratações de computação em nuvem realizadas a partir da vigência deste instrumento e aplica-se aos novos contratos com provedores de serviços de nuvem, os quais precisam estar adequados a essas determinações.

Art. 4º Esta Resolução entra em vigor na data de sua publicação, conforme dados do processo nº 23101.002706/2023-78.

LUÍS EDUARDO BOVOLATO
Reitor



UNIVERSIDADE FEDERAL DO TOCANTINS

POLÍTICA DE COMPUTAÇÃO EM NUVEM DA UNIVERSIDADE FEDERAL DO TOCANTINS (UFT).

Anexo da Resolução nº 101/2023 - Consuni
Aprovada pelo Conselho Universitário em 08 de novembro de 2023.

Palmas-TO,
2023.



UNIVERSIDADE FEDERAL DO TOCANTINS

ANEXO DA RESOLUÇÃO Nº 101/2023 – CONSUNI

POLÍTICA DE COMPUTAÇÃO EM NUVEM DA UNIVERSIDADE FEDERAL DO TOCANTINS (UFT).

Versão 1.0
Palmas/TO, novembro de 2023.

COMITÊ DE GOVERNANÇA DIGITAL (CGD)

Luís Eduardo Bovolato
Reitor

Marcelo Leineker Costa
Vice-Reitor

Eduardo José Cezari
Pró-Reitor de Graduação

Maria Santana Ferreira dos Santos Milhomem
Pró-Reitora de Extensão

Rafael Sanzio Pimenta
Pró-Reitor de Pesquisa e Pós-Graduação

Kherlley Caxias Batista Barbosa
Pró-Reitor de Assistência Estudantil

Eduardo Andrea Lemus Erasmo
Pró-Reitor de Avaliação e Planejamento

Ary Henrique Moraes de Oliveira
Pró-Reitor de Tecnologia da Informação e Comunicação

Michelle Semiguen Lima Duarte
Pró-Reitora de Gestão e Desenvolvimento de Pessoas

Carlos Alberto Moreira de Araújo Júnior
Pró-Reitor de Administração e Finanças

COMITÊ GESTOR DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO (CGTIC)

Ary Henrique Moraes de Oliveira
Pró-Reitor de Tecnologia da Informação e Comunicação

Olivia Tozzi Bittencourt
Diretora de Infraestrutura Tecnológica

Glauco Batista de Sousa
Coordenador de Segurança da Informação

Werley Teixeira Reinaldo
Diretor de Soluções Digitais

Anna Paula de Sousa Parente Rodrigues
Coordenadora de Soluções para a Educação

Samuel Barbosa Costa da Silva
Coordenador de Soluções para a Gestão

EQUIPE DE APOIO TÉCNICO

Aislan Max Gomes Coelho

Analista de Tecnologia da Informação

Jefferson Victor Araújo

Analista de Tecnologia da Informação

Juliano Alves Rios

Analista de Tecnologia da Informação

Junior Fernandes de Oliveira

Técnico de Tecnologia da Informação

Luis Ferreira de Oliveira Junior

Técnico em Tecnologia da Informação

Marluzio Da Silva Leite

Analista de Tecnologia da Informação

Controle de versões:

Versão	Data	Autoria	Tipo de Modificação
1.0	19/05/2023	Coordenação de Segurança da Informação	Versão Inicial do Documento
1.1	30/06/2023	Pró-Reitoria de Tecnologia da Informação e Comunicação	Análise e correção do documento
1.2	31/07/2023	Comitê de Segurança da Informação	Análise e correção do documento
1.3	31/07/2023	Comitê Gestor de Tecnologia da Informação e Comunicação	Aprovação no CGTIC
1.4	31/07/2023	Comitê de Governança Digital	Aprovação no CGD
1.5	07/11/2023	Comissão de Legislação e Normas	Aprovação na CLN/CONSUNI
1.6	08/11/2023	Conselho Universitário	Aprovação no Consuni

Contatos:

Técnico	Telefone	E-mail
Glauco Batista de Sousa	(63) 3229-4034	internet@uft.edu.br
Ediane Dias dos Santos	(63) 3229-4034	protic@uft.edu.br

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 1º Para os fins desta política considera-se:

I. dado pessoal: informação relacionada à pessoa natural identificada ou identificável;

II. dado pessoal sensível: tipo de dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

III. medida técnica: controle relacionado à segurança cibernética, obtido por processo que possibilite a conformidade legal e a confidencialidade, disponibilidade e integridade dos dados pessoais;

IV. medida administrativa: controle organizacional, físico ou procedimental, obtido por processo que possibilite a conformidade legal e a confidencialidade, disponibilidade e integridade dos dados pessoais;

V. relatório de impacto à proteção de dados pessoais (RIPD): documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;

VI. titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VII. controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

VIII. operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, sem vínculo estatutário ou empregatício com o controlador;

IX. tratamento de dados: toda operação realizada com dados pessoais, como as que se referem à coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

X. nuvem privada: infraestrutura de nuvem dedicada para uso exclusivo do órgão e de suas unidades vinculadas, ou de entidade composta por múltiplos usuários, e sua propriedade e seu gerenciamento podem ser da própria organização, de terceiros ou de ambos;

XI. nuvem comunitária: infraestrutura de nuvem dedicada para uso exclusivo de uma comunidade, ou de um grupo de usuários de órgãos ou de entidades não vinculados, que compartilham a mesma natureza de trabalho e obrigações, e sua propriedade e seu gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

XII. nuvem pública (ou externa): infraestrutura de nuvem dedicada para uso aberto de qualquer organização, e sua propriedade e seu gerenciamento podem ser de organizações públicas, privadas ou de ambas;

XIII. nuvem híbrida: infraestrutura de nuvem composta por duas ou mais infraestruturas distintas (privadas, comunitárias ou públicas), que permanecem com

suas próprias características, mas agrupadas por tecnologia padrão que permite interoperabilidade e portabilidade de dados, serviços e aplicações;

XIV. software como um serviço (Software as a Service): modelo de fornecimento (distribuição e comercialização) de software que permite aos usuários se conectar e usar aplicativos baseados em nuvem pela Internet; e

XV. corretor de nuvem (cloud brokers): entidade que gerencia o uso, desempenho e entrega de serviços em nuvem e negocia relacionamentos entre provedores de nuvem e consumidores de nuvem.

Parágrafo único. Doravante, o termo dado pessoal engloba as definições de dado pessoal e dados pessoais sensível, sempre que não determinado especificamente como sensível.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 2º As operações de tratamento de dados deverão observar a boa-fé e os seguintes princípios conforme apresentados no Art. 6º da LGPD:

I. finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;

II. adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;

III. necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV. qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;

V. segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração e comunicação ou difusão não autorizada pelo titular ou por ordem judicial;

VI. prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

VII. responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas;

VIII. não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos.

CAPÍTULO III

OBJETIVO E COMPETÊNCIAS

Art. 3º O objetivo da Política de Computação em Nuvem da Universidade Federal do Tocantins é definir as principais normas, princípios e diretrizes em relação à computação em nuvem, que são aplicáveis à instituição, para garantir o nível de segurança da informação, privacidade e proteção aos dados pessoais determinados pela LGPD:

I. deverão ser observados os requisitos da legislação competente para que as unidades administrativas e acadêmicas da instituição adotem soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia;

II. esta Política de Computação em Nuvem atende ao determinado na Política de Segurança da Informação da Universidade Federal do Tocantins e ao determinado pela legislação competente e define as medidas técnicas e administrativas que deverão ser observadas pelos agentes públicos vinculados à Universidade Federal do Tocantins e por organizações fornecedoras de serviço de computação em nuvem;

III. as medidas técnicas e administrativas devem ser aptas a proteger as informações de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito e considerar a natureza das informações tratadas, as características específicas do tratamento e o estado atual da tecnologia, assim como os princípios previstos em legislação.

CAPÍTULO IV

COMPETÊNCIAS

Art. 4º Compete à alta administração da Universidade:

I. aprovar as presentes determinações do uso seguro de computação em nuvem e divulgá-las às partes interessadas, conforme determinado em normativa legal;

II. instituir uma equipe para elaboração e revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 5º Compete ao Gestor de Segurança da Informação:

I. instituir e coordenar a equipe descrita no item II do art. 6º, responsável pela elaboração e revisões do ato normativo sobre uso seguro de computação em nuvem;

II. supervisionar a aplicação do ato normativo sobre uso seguro de computação em nuvem;

III. assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem, que fornece tais serviços ao órgão ou à entidade, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos;

IV. supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios;

V. comunicar incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância dos incidentes previamente estabelecida; e

VI. encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Art. 6º Compete ao Comitê de Segurança da Informação ou à estrutura equivalente:

I. estabelecer os países nos quais dados e informações custodiados pela administração pública federal poderão ser armazenados em soluções de computação em nuvem;

II. definir os requisitos criptográficos mínimos para o armazenamento de dados e informações, custodiados pela administração pública federal, em soluções de computação em nuvem; e

III. analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

CAPÍTULO V

DOS REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

Art. 7º Em relação à necessidade do uso de recursos criptográficos, os órgãos ou as entidades deverão, no mínimo:

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

II. analisar 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.

Art. 8º Antes de transferir serviços ou informações para um provedor de serviço de nuvem, os órgãos e unidades da Universidade deverão, no mínimo:

I. garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais a LGPD, à presente política, ao sigilo das comunicações privadas e dos registros as seguintes operações:

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

b. de comunicações realizadas 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 LGPD, dos seguintes itens:

a. o tipo de informação a ser migrada;

b. o fluxo de tratamento dos dados que podem ser afetados com a adoção da solução;

c. o valor dos ativos envolvidos; e

d. os benefícios da adoção de uma solução de computação em nuvem, em relação aos riscos de segurança e privacidade referentes à disponibilização de informações e serviços a um terceiro.

III. definir o modelo de serviço e de implementação de computação em nuvem que será 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 de entidades;

V. avaliar quais informações serão hospedadas na nuvem, considerando:

a. o processo de classificação da informação de acordo com a legislação e com a Política de Classificação e Compartilhamento de Dados Pessoais da UFT;

b. o valor do ativo de informação;

c. os controles de acessos físico e lógico relativos à segurança da informação;

d. o modelo de serviço e de implementação de computação em nuvem;

e. 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

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

Art. 9º Em relação ao gerenciamento de identidades e de registros, os órgãos, as unidades, conforme suas incumbências e responsabilidades, deverão no mínimo:

I. negar ao provedor de serviço de nuvem permissão de uso e acesso direto ao ambiente de autenticação do órgão ou da entidade;

II. armazenar os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações, por um ano, no ambiente do provedor de serviço de nuvem ou em ambiente próprio controlado, à critério do órgão ou da entidade contratante;

III. manter em ambiente próprio controlado, pelo período de um ano ou período mínimo que esteja em conformidade com a legislação vigente, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informação sobre sessões e transações recebidos do provedor de serviço de nuvem;

IV. capacitar a equipe de segurança da informação para acessar e utilizar os registros gerados pelo provedor de serviço de nuvem;

V. adotar o padrão de identidade federada para permitir o uso de tecnologia single sign-on no processo de autenticação de seus usuários no provedor de serviço de nuvem;

VI. 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 uma alternativa que aumente o grau de segurança no processo de autenticação de seus usuários no provedor de serviço de nuvem.

VII. 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.

Art. 10. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, os órgãos e unidades da Universidade, em conjunto com o provedor de serviço de nuvem, deverão estabelecer, no mínimo, as seguintes ações:

I. garantir que o ambiente contratado seja protegido de usuários externos do serviço em nuvem e de pessoas não autorizadas e implementar controles de segurança da informação de forma a propiciar o isolamento adequado dos recursos utilizados pelos diferentes órgãos ou entidades da administração pública federal e por outros usuários do serviço em nuvem;

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;

III. garantir a separação de todos os recursos utilizados pelo Provedor de Serviço de Nuvem daqueles recursos utilizados pela administração interna do órgão ou da entidade; e

IV. avaliar os riscos associados à execução de softwares proprietários a serem instalados no serviço de nuvem.

Art. 11. Em relação ao gerenciamento da nuvem, os órgãos e unidades da Universidade deverão, no mínimo:

I. capacitar a equipe responsável por esse gerenciamento nas tecnologias utilizadas pelo provedor de serviço de nuvem;

II. exigir que o provedor de serviço de nuvem documente e comunique seus recursos, papéis e responsabilidades de segurança da informação para o uso de seus serviços em nuvem;

III. elaborar uma matriz de responsabilidades que inclua obrigações e responsabilidades próprias; e

IV. elaborar um processo de tratamento de incidentes junto ao provedor de serviço de nuvem e comunicá-lo à equipe responsável pelo gerenciamento da nuvem.

Art. 12. Em relação ao tratamento da informação em ambiente de computação em nuvem, os órgãos e unidades da Universidade, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais LGPD e a Política de Classificação e Compartilhamento de Dados Pessoais da UFT, deve observar as seguintes diretrizes:

I. informação sem restrição de acesso poderá ser tratada em ambiente de nuvem, considerada a legislação e os riscos de segurança da informação;

II. informação classificada em grau de sigilo e documento preparatório que possa originar informação classificada não poderão ser tratados em ambiente de computação em nuvem; e

III. poderão ser tratados em ambiente de computação em nuvem, observados os riscos de segurança da informação e a legislação vigente:

a. a informação com restrição de acesso prevista na legislação, conforme a Política de Classificação e Compartilhamento de Dados Pessoais da UFT;

- b. o material de acesso restrito regulado pelo próprio órgão ou pela entidade;
- c. a informação pessoal relativa à intimidade, vida privada, honra e imagem; e
- d. o documento preparatório não previsto no inciso II do caput.

Art. 13. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo órgão ou pela entidade, 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;

III. informação com restrição de acesso prevista na legislação e o documento preparatório não previsto no inciso II do caput art. 13, bem como suas cópias atualizadas de segurança, não poderão ser tratados fora do território brasileiro, conforme legislação aplicável; e

IV. no caso de dados pessoais, deverão ser observadas as orientações previstas na legislação competente, à proteção de dados e privacidade, e o Programa de Governança em Privacidade da Universidade.

CAPÍTULO VI

DAS CLÁUSULAS CONTRATUAIS

Art. 14. O instrumento contratual a ser firmado com um provedor de serviço de nuvem para a prestação do serviço de computação em nuvem deve conter dispositivos que tratam dos requisitos estabelecidos nesta política e, no mínimo, os seguintes procedimentos de segurança:

I. termo de confidencialidade que impeça o provedor de serviço de nuvem de usar, transferir e liberar dados, sistemas, processos e informações do órgão ou da entidade para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II. garantia da exclusividade de direitos, por parte do órgão ou da entidade, sobre todas as informações tratadas durante o período contratado, incluídas eventuais cópias disponíveis, tais como backups de segurança;

III. proibição do uso de informações do órgão ou da entidade pelo provedor de serviço de nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado;

IV. conformidade da política de segurança da informação do provedor de serviço de nuvem com a legislação brasileira;

V. devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem aos órgãos ou às entidades contratantes ao término do contrato; e

VI. eliminação, por parte do provedor de serviço de nuvem, ao término do contrato, de qualquer dado, informação ou sistema do órgão ou entidade sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados.

CAPÍTULO VII

DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 15. Para que esteja habilitado a prestar serviços de computação em nuvem para os órgãos e unidades da Universidade, o provedor de serviço de nuvem deverá cumprir, no mínimo, os seguintes requisitos:

I. possuir metodologia de gestão de riscos, elaborada em conformidade com as melhores práticas e com a legislação, bem como realizar o gerenciamento de riscos descrito no inciso II do art. 9º;

II. implementar práticas de fortalecimento dos mecanismos de virtualização, que devem incluir, no mínimo, os seguintes procedimentos:

a. desabilitar ou remover todas as interfaces, portas, dispositivos ou serviços desnecessários executados pelo sistema operacional;

b. configurar com segurança todas as interfaces de rede e áreas de armazenamento virtuais;

c. estabelecer limites para a utilização dos recursos de máquina virtual (Virtual Machine - VM);

d. manter todos os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais;

e. validar a integridade das operações de gerenciamento de chaves criptográficas;

f. possuir controles que permitam aos usuários autorizados do órgão ou da entidade acessarem os registros de acesso administrativo do monitor de máquina virtual - Hypervisor;

g. habilitar o registro completo do Hypervisor; e

h. suportar o uso de máquinas virtuais confiáveis (Trusted VM) fornecidas pelo órgão ou pela entidade, que estejam em conformidade com as políticas e práticas de fortalecimento de redes exigidas ao provedor de serviço de nuvem.

III. em relação ao gerenciamento de identidades e registros:

a. possuir procedimentos de controle de acesso que abordam a transição entre as funções, os limites e controles dos privilégios dos usuários e os controles de utilização das contas de usuários;

b. impor mecanismo de autenticação que exija tamanho mínimo, complexidade, duração e histórico de senhas de acesso;

c. suportar tecnologia single sign-on para autenticação;

d. suportar mecanismos de autenticação multifator ou outra alternativa que aumente o grau de segurança no processo de autenticação de usuários do órgão ou da entidade no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;

e. permitir ao órgão ou à entidade gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem; e

f. atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo órgão ou pela entidade em seus processos de autenticação, controle de acesso, contabilidade e de registro (formato, retenção e acesso).

IV. em relação à segurança de aplicações web disponibilizadas no ambiente de nuvem:

- a. utilizar firewalls especializados na proteção de sistemas e aplicações;
- b. desenvolver código web em conformidade com as melhores práticas de desenvolvimento seguro e com os normativos existentes;
- c. utilizar melhores práticas de segurança de sistemas operacionais e de aplicações;
- d. realizar periodicamente testes de penetração de redes e de aplicações;

e

- e. possuir um programa de correção de vulnerabilidades.

V. possuir processos de gestão de continuidade de negócios e de gestão de mudanças, em conformidade com os normativos existentes e com as melhores práticas nessas áreas;

VI. possuir um plano de recuperação de desastres que estabeleça procedimentos de recuperação e de restauração de plataforma, infraestrutura, aplicações e dados após incidentes de perda de dados;

VII. estabelecer um canal de comunicação seguro utilizando, no mínimo, Secure Sockets Layer/Transport Layer Security (SSL/TLS);

VIII. utilizar um padrão de encriptação seguro, conforme padrão internacional reconhecidamente aceito, que possa ser implementado com chaves de encriptação geradas e armazenadas pelo órgão ou pela entidade;

IX. disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do órgão ou da entidade;

X. em relação à segregação de dados:

- a. isolar utilizando separação lógica, todos os dados e serviços do órgão ou da entidade de outros clientes de serviço em nuvem;
- b. segregar o tráfego de gerenciamento do tráfego de dados do órgão ou da entidade; e implementar dispositivos de segurança entre zonas;

XI. possuir procedimentos em relação ao descarte de ativos de informação e de dados, que assegurem:

- a. sanitizar ou destruir, de modo seguro, os dados existentes nos dispositivos descartados por meio da utilização de métodos que estejam em conformidade com os padrões estabelecidos para a conduta e as melhores práticas;

- b. destruir, de modo seguro, ativo de informação no fim do ciclo de vida ou considerado inservível, com o fornecimento de um Certificado de Destruição de Equipamento Eletrônico (Certificate of Electronic Equipment Destruction - CEED) e discriminar os ativos que foram reciclados, bem como o peso e os tipos de materiais obtidos em virtude do processo de destruição; e

- c. armazenar de modo seguro, ativos de informação a serem descartados, em ambiente com acesso físico controlado, com registro de toda movimentação de entrada e saída de dispositivos.

XII. notificar, imediatamente, aos órgãos ou às entidades incidente cibernético contra os serviços ou dados sob sua custódia;

XIII. possuir procedimentos necessários para preservação de evidências, conforme legislação;

XIV. demonstrar estar em conformidade com os padrões de segurança de nuvem, por meio de auditoria anual Service and Organization Controls 2 (SOC 2), conduzida por um auditor; e

XV. independente com a apresentação dos relatórios de tipo I e tipo II. O Relatório de Conformidade SOC 2 para Computação em nuvem é uma avaliação independente realizada por uma empresa de auditoria externa para verificar a conformidade de um provedor de serviços em nuvem com os critérios estabelecidos pelo AICPA (American Institute of Certified Public Accountants) no padrão SOC 2. Este padrão concentra-se em cinco princípios fundamentais: Segurança, Disponibilidade, Integridade de Processamento, Confidencialidade e Privacidade.

CAPÍTULO VIII

DA UTILIZAÇÃO DE CLOUD BROKERS/CORRETORES DE NUVEM

Art. 16. O cloud broker (corretor de nuvem) deverá atuar como integrador dos serviços de computação em nuvem entre o órgão ou unidade da Universidade e dois ou mais provedores de serviço de nuvem.

Art. 17. Caso o órgão ou a entidade contrate por meio do cloud broker plataforma de gestão multi nuvem para realizar procedimentos de provisionamento e orquestração do ambiente, é necessário que a ferramenta possua, no mínimo:

I. em relação às funcionalidades de provisionamento e orquestração de multi nuvem:

- a. um único portal integrado de provisionamentos para o usuário final;
- b. utilização de modelos de provisionamento;
- c. automação segura de provisionamento simultâneo e utilização, no que couber, ferramentas de código aberto e interoperáveis;
- d. fluxos de trabalho de orquestração baseada em eventos; e
- e. soluções seguras integradas de criação de infraestrutura por código – IaaS.

II. em relação às funcionalidades de monitoramento e análise em multi nuvem:

- a. relatórios de monitoramento de desempenho de recursos na nuvem;
- b. coleta e monitoramento de registros; e
- c. procedimentos de monitoramento de alertas.

III. em relação às funcionalidades de inventário e classificação em multi nuvem:

- a. inventário de recursos na nuvem;
- b. procedimentos de segurança para configuração de recursos na plataforma de gestão multi nuvem; e
- c. detecção de recursos sem etiqueta.

IV. em relação às funcionalidades de gerenciamento de segurança, conformidade e identidade:

- a. mecanismos de single sign-on e de autenticação multifator das plataformas em nuvem;

- b. gerenciamento seguro de usuários e de grupos de usuários;
- c. gerenciamento de segurança dos recursos;
- d. notificações de eventos de alerta multicanal;
- e. gerenciamento de identidade e acesso - (Identity and Access Management/IAM); e
- f. registros de atividade da plataforma em nuvem.

Parágrafo único. O cloud broker poderá utilizar ferramentas de Software as a Service (SaaS) comum de mercado, desde que não haja risco de dependência tecnológica para disponibilizar essa plataforma.

Art. 18. O cloud broker é o responsável por garantir que os provedores de serviço de nuvem que ele representa:

- I. cumpram todos os requisitos previstos nesta Política e na legislação brasileira; e
- II. operem de acordo com as melhores práticas de segurança.

Parágrafo único. O órgão ou a entidade deverá prever no instrumento contratual que o cloud broker poderá ser responsabilizado, civil e administrativamente, por qualquer desconformidade nos provedores que ele representa.

Art. 19. A apresentação dos relatórios de tipo I e tipo II da auditoria SOC 2, comprovada a conformidade com os padrões de segurança em nuvem, é condição essencial, tanto para habilitar a participação em processo licitatório, como para renovar o contrato de prestação de serviço em nuvem com órgãos ou entidades da administração pública federal.

Parágrafo único. Na hipótese de utilização de cloud broker, esse será o responsável por apresentar os relatórios de tipo I e tipo II da auditoria SOC 2 de todos os provedores de serviço de nuvem que ele representa.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 20. As violações à segurança da informação estão sujeitas às sanções previstas em lei. A ausência de providências ou a não observância das determinações legais pode acarretar em repercussões negativas à UFT e em sanções administrativas, civis e penais, isolada ou cumulativamente, aos responsáveis, nos termos da legislação aplicável, assegurado aos envolvidos o contraditório e a ampla defesa.

Art. 21. Em função da capacidade dos provedores de serviço de nuvem implementar atualizações relacionadas à segurança da informação em seus produtos e serviços, a presente política poderá ser revisada 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; e
- II. atualizar periodicamente os processos internos de gestão de riscos de segurança da informação.

Art. 22. Esta Resolução entra em vigor na data de sua publicação, conforme dados do processo nº 23101.002706/2023-78.

Palmas/TO, 08 de novembro de 2023.

Luís Eduardo Bovolato
Reitor