

TRIBUNAL DE JUSTIÇA - ATOS DO PRESIDENTE

PORTARIA 01385/2025

Disponibilização: 30/05/2025 às 15h11m

PORTARIA Nº 1385/2025-GABPRESI

Dispõe sobre as diretrizes de uso seguro de computação em nuvem no âmbito do Poder Judiciário do Estado do Ceará.

O PRESIDENTE DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ (TJCE) , no uso de suas atribuições legais e regimentais,

CONSIDERANDO os termos da Resolução do Conselho Nacional de Justiça (CNJ) nº 370/2021, que instituiu a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD) e estabeleceu as diretrizes para sua governança, gestão e infraestrutura de TIC;

CONSIDERANDO o determinado na Lei Geral de Proteção de Dados Pessoais – Lei Federal nº 13.709/2018 (LGPD);

CONSIDERANDO o que está previsto no processo de Segurança da Informação (SI), Gerir Segurança dos Serviços em Nuvem / Elaborar Normativos de Segurança da Informação;

CONSIDERANDO os termos da Resolução do Órgão Especial do TJCE nº 15/2023 (DJe 6.7.2023), que atualiza a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará;

CONSIDERANDO o disposto na Portaria nº 652/2025 (DJE 14.3.2025), que dispõe sobre as diretrizes de Tratamento, Classificação e Sigilo da Informação no âmbito do Poder Judiciário do Estado do Ceará;

CONSIDERANDO os termos da Portaria do Conselho Nacional de Justiça nº 162/2021, que aprovou protocolos e manuais criados pela Resolução-CNJ nº 396/2021, a qual instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

CONSIDERANDO as boas práticas de Governança de Tecnologia da Informação que visam a garantir a disponibilidade e a integridade de sistemas, aplicativos, dados e documentos digitais do Poder Judiciário do Estado do Ceará;

CONSIDERANDO requisitos e obrigações para uso seguro de computação em nuvem, que prevejam a realização de auditoria relativa à conformidade dos requisitos de segurança da informação e privacidade previstos pela contratação, implementem controles criptográficos, registros de *logs*, políticas de segurança da informação e privacidade;

RESOLVE:

Art. 1º Definir, no âmbito do Poder Judiciário do Estado do Ceará, as diretrizes de uso seguro de computação em nuvem, englobando os respectivos serviços de operação e gerenciamento.

Parágrafo único. O conjunto das diretrizes de que trata o *caput* deste artigo compõe a Política de Computação em Nuvem (PCN) do TJCE.

Art. 2º A Política de Computação em Nuvem do TJCE observará os princípios, objetivos e diretrizes estabelecidos nesta Portaria, bem como as disposições constitucionais, legais e regimentais vigentes.

Art. 3º As determinações da PCN aplicam-se a novas contratações de computação em nuvem realizadas a partir da data de publicação desta Portaria.

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Art. 4º Para os fins desta norma 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 normativa 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 normativa 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 - alta gestão: Presidência e Vice-Presidência do Tribunal de Justiça do Estado do Ceará e a Corregedoria-Geral da Justiça do Estado do Ceará;

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

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

IX - 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;

X - 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;

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

XII - 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. Sua propriedade e gerenciamento podem ser de organizações da comunidade, de terceiros ou de ambos;

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

XIV - 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.

Parágrafo único. Doravante, o termo “dado pessoal” englobará as definições de dado pessoal e dado pessoal sensível, sempre que não determinado especificamente como sensível.

CAPÍTULO II

DOS PRINCÍPIOS

Art. 5º As operações de tratamento de dados deverão observar a boa-fé e os seguintes princípios:

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.

CAPÍTULO III

DO OBJETIVO E DAS COMPETÊNCIAS

Art. 6º O objetivo da PCN é definir as principais normas, princípios, objetivos e diretrizes em relação à computação em nuvem, que são aplicáveis ao TJCE, para garantir o nível de segurança da informação, privacidade e proteção aos dados pessoais determinados pela legislação competente.

§ 1º Deverão ser observados os requisitos da legislação competente para que se adotem soluções de computação em nuvem de forma segura, com o objetivo de elevar o nível de proteção das informações no uso dessa tecnologia.

§ 2º A PCN deve atender às determinações constantes da Política de Segurança do TJCE e da legislação competente e define as medidas técnicas e administrativas que deverão ser observadas pelos agentes públicos vinculados ao TJCE e por fornecedoras de computação em nuvem.

§ 3º 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.

Art. 7º Compete à alta gestão do TJCE aprovar as presentes determinações do uso seguro de computação em nuvem e divulgá-las às partes interessadas, conforme determinado em normativa legal.

CAPÍTULO IV

DOS REQUISITOS PARA A ADOÇÃO SEGURA DE COMPUTAÇÃO EM NUVEM

Art. 8º Os requisitos criptográficos mínimos para o armazenamento de dados e informações, em soluções de computação em nuvem, devem atender às determinações da Política Nacional de Segurança da Informação - PNSI.

Parágrafo único. Em relação à necessidade do uso de recursos criptográficos, no mínimo deverão ser observados:

I - que os dados da organização sejam tratados e armazenados de acordo com a legislação;

II - a necessidade de criptografar dados com base nos requisitos legais, nos riscos, no nível de criticidade, nos custos e nos benefícios; e

III - a utilização, sempre que possível, de chaves de encriptação baseadas em hardware.

Art. 9º Antes de transferir serviços ou informações para um provedor de serviço de nuvem, o TJCE deverá, no mínimo:

I - garantir que estejam alinhadas à legislação brasileira e aos direitos à privacidade, à proteção dos dados pessoais, à presente Portaria, 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 realizada 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 legislação, 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 Norma de Tratamento e Classificação da Informação do TJCE;
- 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;

VI - 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

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

Art. 10. Em relação ao gerenciamento de identidades e de registros, o TJCE deverá:

I - negar ao provedor de serviço de nuvem (*CSP - Cloud Service Provider*) permissão de uso e acesso direto ao ambiente de autenticação do TJCE. Essa restrição não alcança a aplicação do TJCE rodando no ambiente do provedor, incluindo serviços de autenticação oferecidos pelo provedor, como o AWS Cognito, desde que devidamente controlados pelo TJCE;

II - manter em ambiente próprio controlado, pelo período de cinco anos, os registros de todos os acessos, incidentes e eventos cibernéticos, incluindo informações sobre sessões e transações, recebidos do provedor de serviço de nuvem. Para garantir a disponibilidade e integridade desses registros, o TJCE deverá estabelecer rotinas de sincronização em tempo real ou quase tempo real com o ambiente do provedor;

III - exigir do provedor de serviço de nuvem que registre todos os acessos, incidentes e eventos cibernéticos, incluídas informações sobre sessões e transações, e que armazene esses registros por um período mínimo de 1 (um) ano, garantindo o envio contínuo desses registros ao ambiente próprio do TJCE;

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 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 mínimo de 1 (um) ano, todos os registros de que trata a alínea a.

Art. 11. Em relação à segregação de dados e à separação lógica em ambientes de computação em nuvem, o TJCE, em conjunto com o provedor de serviço de nuvem, deverá 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 TJCE; e

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

Art. 12. Em relação ao gerenciamento da nuvem, o TJCE deverá, 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. 13. Em relação ao tratamento da informação em ambiente de computação em nuvem, o TJCE, além de cumprir as orientações contidas na legislação sobre proteção de dados pessoais e a Norma de Tratamento e Classificação da Informação do TJCE, 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 ou documento preparatório que possa originar informação classificada deverá ser tratada com o mais alto nível de segurança, com possibilidade de uso em ambiente de nuvem desde que sejam implementados controles robustos de criptografia e de segregação de acesso, compatíveis com as normas e orientações de segurança da informação. Caso não seja possível garantir tais controles no ambiente de nuvem, o tratamento deverá ser realizado em ambiente controlado e protegido localmente; 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 Norma de Tratamento e Classificação da Informação do TJCE;

- b. o material de acesso restrito regulado pelo TJCE;
- 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. 14. Os dados, metadados, informações e conhecimentos produzidos ou custodiados pelo TJCE, 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*, do 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.

Parágrafo único. Havendo necessidade, a Presidência poderá redefinir o limite geográfico previsto no *caput* deste artigo, ouvindo previamente o Comitê de Governança da Segurança da Informação, de Crises Cibernéticas e de Proteção de Dados Pessoais.

CAPÍTULO V

DAS CLÁUSULAS CONTRATUAIS

Art. 15. O instrumento contratual a ser firmado com um provedor de serviço de nuvem, diretamente ou por meio de um integrador, para a prestação do serviço de computação em nuvem deve conter dispositivos que tratem dos requisitos estabelecidos nesta Política e, no mínimo, os seguintes procedimentos de segurança:

I - termo de confidencialidade que impeça tanto o provedor de serviço de nuvem quanto o integrador e seus parceiros de usar, transferir, compartilhar e liberar dados, sistemas, processos e informações do TJCE para empresas nacionais, transnacionais, estrangeiras, países e governos estrangeiros;

II - garantia da exclusividade de direitos, por parte do TJCE, 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 TJCE pelo provedor de serviço de nuvem, pelo integrador ou seus parceiros 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, do integrador e de seus parceiros com a legislação brasileira;

V - devolução integral dos dados, informações e sistemas sob custódia do provedor de serviço de nuvem, do integrador e de seus parceiros ao TJCE ao término do contrato;

VI - eliminação, por parte do provedor de serviço de nuvem, do integrador e de seus parceiros, ao término do contrato, de qualquer dado, informação ou sistema do TJCE sob sua custódia, observada a legislação que trata da obrigatoriedade de retenção de dados;

Parágrafo único. A empresa contratada deve apresentar evidências que comprovem tal eliminação.

CAPÍTULO VI

DOS REQUISITOS DO PROVEDOR DE SERVIÇO DE NUVEM

Art. 16. Para que esteja habilitado a prestar serviços de computação em nuvem para o TJCE, 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. permitir que o cliente mantenha os sistemas operacionais e as aplicações em execução na máquina virtual em suas versões mais atuais, conforme a responsabilidade do cliente;
- e. validar a integridade das operações de gerenciamento de chaves criptográficas;
- f. possuir controles que permitam aos usuários autorizados do TJCE acessarem os registros de acesso administrativo do serviço, conforme aplicável;
- g. habilitar o registro completo das atividades relevantes no ambiente de nuvem;
- h. suportar a implementação de instâncias de máquinas virtuais fornecidas pelo TJCE, em conformidade com as políticas e práticas de segurança exigidas ao provedor de serviço de nuvem;

III - em relação ao gerenciamento de identidades e registros:

- a. possuir procedimentos de controle de acesso que abordem 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 TJCE no provedor de serviço de nuvem, de acordo com nível de criticidade da informação;
- e. permitir ao TJCE gerenciar as próprias identidades, inclusive criação, atualização, exclusão e suspensão no ambiente fornecido pelo provedor de serviço de nuvem;
- f. atender aos requisitos legais, às melhores práticas de segurança e a outros critérios exigidos pelo TJCE 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. 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 TJCE;

IX - disponibilizar facilidades que possibilitem a aplicação de uma proteção criptográfica própria do TJCE;

X - em relação à segregação de dados:

a. isolar, utilizando separação lógica, todos os dados e serviços do TJCE de outros clientes de serviço em nuvem;

b. segregar o tráfego de gerenciamento do tráfego de dados do TJCE;

c. 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;

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 de saída de dispositivos;

XII - notificar, imediatamente, ao TJCE 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 independente, com a apresentação dos relatórios de tipo I e tipo II.

CAPÍTULO VII

DA UTILIZAÇÃO DE *CLOUD BROKERS*

Art. 17. O *cloud broker* deverá atuar como integrador dos serviços de computação em nuvem entre o TJCE e dois ou mais provedores de serviço de nuvem.

Art. 18. Caso o TJCE contrate por meio do *cloud broker* plataforma de gestão multinuvem 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 multinuvem:

- 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 - IaC;

II - em relação às funcionalidades de monitoramento e análise em multinuvem:

- 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 multinuvem:

- a. inventário de recursos na nuvem;
- b. procedimentos de segurança para configuração de recursos na plataforma de gestão multinuvem;
- 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 - 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. 19 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 portaria 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. 20 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 VIII

DAS DISPOSIÇÕES FINAIS

Art. 21. As violações à segurança da informação estão sujeitas às sanções previstas em lei. A ausência de providências ou a não observância das determinações legais e daquelas contidas nesta Portaria pode acarretar 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. 22. Em função da capacidade de os provedores de serviço de nuvem implementarem 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. 23. Esta Portaria entra em vigor na data de sua publicação.

REGISTRE-SE, PUBLIQUE-SE E CUMPRA-SE. GABINETE DA PRESIDÊNCIA DO TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ , em Fortaleza, aos 29 dias de maio de 2025.

Desembargador Heráclito Vieira de Sousa Neto

Presidente do Tribunal de Justiça do Estado do Ceará

Para visualizar a matéria completa, acesse o link <https://djea-con.tjce.jus.br/materias/132141> ou realize a leitura do QR-Code ao lado.

