MINISTÉRIO DA EDUCAÇÃO
SECRETARIA DE EDUCAÇÃO PROFISSIONAL E TECNOLÓGICA
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DO SERTÃO PERNAMBUCANO
REITORIA

RESOLUÇÃO Nº 24 DO CONSELHO SUPERIOR, DE 23 DE JUNHO DE 2025.

APROVA a Norma Complementar 07 do Comitê Gestor de Segurança da Informação, a qual estabelece a estratégia de adoção e uso de serviços e plataformas em nuvem pelo Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IFSertãoPE.

O Presidente do Conselho Superior do Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano, no uso de suas atribuições legais, conforme Decreto Presidencial de 16/05/2024, publicado no D.O.U. nº 95, de 17/05/2024, Seção 2, RESOLVE, *Ad Referendum*:

Art. 1º APROVAR a Norma Complementar 07 do Comitê Gestor de Segurança da Informação, a qual estabelece a estratégia de adoção e uso de serviços e plataformas em nuvem pelo Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano - IFSertãoPE.

Art. 2º Esta resolução entra em vigor a partir da data da sua publicação.

gov.br
Documento assinado digitalmente
JEAN CARLOS COELHO DE ALENCAR
Data: 23/06/2025 13:35:09-0300
Verifique em https://validar.iti.gov.br

JEAN CARLOS COELHO DE ALENCAR
Presidente do Conselho Superior

PUBLICADO NO SITE INSTITUCIONAL EM: 23/06/2025.

NORMA COMPLEMENTAR 07

Estabelece a estratégia de adoção e uso de serviços e plataformas em nuvem pelo Instituto Federal de Educação, Ciência e Tecnologia do Sertão Pernambucano (IFSertãoPE).

OBJETIVO

Art. 1º. Estabelecer diretrizes no âmbito do IFSertãoPE, para a contratação e uso dos serviços de Computação em Nuvem pública (Cloud Computing), em conformidade com o IN PR/GSI nº 5, de 30 de Agosto de 2021, com a Resolução IFSertãoPE Nº 13 de 22 de junho de 2016 (POSIC), com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD) e com a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet); visando à proteção dos dados pessoais, integridade das informações, e a segurança dos ativos digitais.

Art. 2º. Os objetivos a serem alcançados com o uso dos serviços de Computação em Nuvem devem estar alinhados com os objetivos estratégicos de TIC do IFSertãoPE, que são:

I - Promover a Contínua Capacitação Técnica e Gerencial do Pessoal de TIC (OE1);

II - Aprimorar as Práticas de Gestão e Governança de TIC (OE2);

III - Promover a Segurança da Informação e Comunicação (OE3);

IV - Prover Serviços e Infraestrutura de TIC apropriada às atividades Administrativas e Educacionais (OE4);

ESCOPO

Art. 3º. O escopo desse documento se aplica às contratações de software e serviço de computação em nuvem estabelecidos na IN SGD/ME nº 94, de 23 de dezembro de 2022, regidos pela Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023, e pela IN PR/GSI nº 5, de 30 de Agosto de 2021 e suas respectivas revisões. Os termos utilizados neste documento são os mesmos definidos nas portarias supracitadas.

DEFINIÇÕES

Art. 4º. Para o uso de nuvem pública, a organização adota os seguintes princípios e definições utilizados na Portaria SGD/MGI nº 5.950, de 26 de outubro de 2023:

I - Nuvem Pública: Serviços de computação em nuvem fornecidos por terceiros em ambientes compartilhados, incluindo armazenamento, processamento, banco de dados, redes e outros serviços;

II - Dado Pessoal: Qualquer informação relacionada a uma pessoa natural identificada ou identificável, conforme definido pela LGPD;

III - Dado Sensível: Dado pessoal sobre origem racial, religiosa, opinião política, saúde, genética, entre outros dados que exigem tratamento diferenciado;

IV - Segurança e Privacidade: Garantir que os dados sejam armazenados de forma segura, respeitando a confidencialidade e privacidade;

V- Conformidade Legal: Cumprir as diretrizes da LGPD e normativas governamentais relacionadas ao armazenamento e tratamento de dados;

VI - Minimização de Dados: Limitar o armazenamento de dados ao necessário para a finalidade específica, reduzindo riscos;

VII - Transparência e Responsabilidade: Assegurar que as atividades relacionadas ao uso de nuvem pública sejam transparentes e que todas as partes envolvidas compreendam suas responsabilidades;

VIII - Localização dos dados: Refere-se a localização geográfica (país, estado ou cidade) onde os dados são armazenados;

IX - Gestão unificada: Refere-se ao estabelecimento de contas administrativas de gestão de recursos e soluções centralizadas na reitoria, de maneira que a equipe técnica da reitoria possa prestar auxílio às equipes dos campi quando necessário;

X - Gestão compartilhada: Os ambientes centralizados devem permitir que as equipes responsáveis de cada campus tenham plena disponibilidade e autonomia administrava na gestão dos ambientes, sem necessidade de consulta prévia à reitoria para quaisquer ações administrativas, desde que não excluam o acesso da equipe da reitoria ao ambiente;

XI - Provedor de Nuvem: Pessoa Física, jurídica, pública ou privada, ou organização que oferece consultoria, plataformas, infraestrutura, aplicativos, serviços de armazenamento ou ambientes de tecnologia da informação, atuando como intermediária ou facilitadora na seleção e adoção de soluções de computação em nuvem em nome de uma organização, seja como terceira parte ou como detentora direta dos recursos;

DIRETRIZES GERAIS

Seção I

Das necessidades do negócio

Art. 5º. São considerados requisitos de TIC, os itens necessários para o atendimento dos Objetivos Estratégicos (OE1 e OE5) do Plano Diretor de TIC (PDTIC 2025 – 2026).

Art. 6º. São elegíveis para a contratação de serviço em nuvem, quaisquer soluções que sejam aderentes às necessidades de negócio, tecnológicas ou conforme demonstração de eficiência operacional e administrativa, e em respeito às normativas existentes.

§ 1º Os Campi poderão realizar contratação de serviços e soluções de nuvem pública.

I - No caso de contratações realizadas pelos Campi, estes deverão realizar consulta junto a equipe técnica de TI da Reitoria a respeito da contratação.

II - O objetivo desta consulta é o alinhamento da contratação do campus às diretrizes e a gestão unificada e distribuída junto a reitoria, evitando que diversos centros de administração sejam criados e de maneira a garantir a continuidade do ambiente dos campi.

III - Os Campi deverão balizar contratações de soluções de nuvem pública neste documento.

a) No caso de ambientes de nuvem pública de campi já existem de maneira prévia a publicação deste documento, a equipe técnica de TI do campus deverá entrar em contato com a equipe técnica de TI da Reitoria para analisar a possibilidade de unificação de ambientes de gestão e administração compartilhada, de maneira a garantir a continuidade do negócio.

b) A gestão compartilhada do ambiente não isenta a equipe técnica responsável pela manutenção do alvo em relação aos princípios da segurança da informação e operação dos serviços hospedados na plataforma de nuvem.

Seção II

Dos requisitos de continuidade dos serviços

Art. 7º. O Provedor de Serviços em Nuvem, visando a perenidade e resiliência do negócio da CONTRATANTE, respeitando o disposto na Portaria 5.950/2023, devem:

I - Garantir o atendimento aos mais altos padrões de certificação ANSI/TIA/EIA 942, com disponibilização de certificações da Uptime Institute;

II - Fornecer opções de redundância em mais de uma localização geográfica dentro do país ou fora dele, conforme classificação do dado;

III - Prover soluções de software que permitam a interoperabilidade dos serviços;

IV - Prover logs de auditoria, com registro de acessos físicos e lógicos aos sistemas da instituição nele vinculados ou que estejam na dependência de sistemas de nuvem.

Seção III

Dos requisitos de segurança do provedor de nuvem

Art. 8º. O Provedor de Serviços em Nuvem deve estar em conformidade com os requisitos de segurança definidos na instrução normativa IN PR/GSI nº 5, de 30 de Agosto de 2021, incluindo a manutenção de controles de acesso e proteção de dados.

Art. 9º. O Provedor de Serviços em Nuvem deve estar em conformidade com os requisitos de segurança, privacidade e proteção de dados pessoais, em conformidade com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD) e demais normas de segurança do governo federal.

Art. 10º. O Provedor de Serviços em Nuvem deve apresentar relatórios de auditoria sobre conformidade e segurança, conforme IN PR/GSI nº 5, de 30 de Agosto de 2021.

Seção IV

Da classificação e proteção de dados

Art. 11º. Dados, informações pessoais sensíveis e informações classificadas devem ser protegidos por medidas adicionais de segurança, incluindo criptografia e controles de acesso.

Art. 12º. Todos os dados armazenados e processados em ambientes de nuvem devem ser classificados segundo a sua sensibilidade e valor, conforme as diretrizes da Política de Segurança da Informação da instituição, em conformidade com a IN PR/GSI nº 5, de 30 de Agosto de 2021.

Seção V

Da localização dos dados

Art. 13º. De acordo com a IN PR/GSI nº 5, de 30 de Agosto de 2021, é obrigatório que, pelo menos, uma cópia atualizada dos dados, metadados, informações e conhecimentos, produzidos ou custodiados pela instituição e transferidos para o Provedor de Serviços em Nuvem, seja mantida em território nacional.

Art. 14º. A transferência e o armazenamento de dados pessoais e pessoais sensíveis, fora do Brasil, devem estar em conformidade com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), e é necessário garantir que a segurança dos dados seja equivalente àquela oferecida em território nacional.

Seção VI

Dos requisitos de armazenamento

Art. 15º. Dados pessoais e pessoais sensíveis devem ser armazenados em conformidade com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), com garantias de que o Provedor de Serviços em Nuvem utiliza mecanismos adequados de criptografia e controle de acesso.

Art. 16º. Os dados passíveis de serem armazenados e processados em ambientes de nuvem, devem estar em conformidade com as diretrizes da Política de Segurança da Informação da instituição e com a IN PR/GSI nº 5, de 30 de Agosto de 2021.

Seção VII

Dos controles de acesso e autenticação

Art. 17º. Somente usuários autorizados poderão ter acesso aos mecanismos e sistemas de gestão dos ambientes em nuvem.

Art. 18º. O acesso aos mecanismos e sistemas de gestão dos ambientes em nuvem deverá ter como base os princípios do modelo zero trust.

Art. 19º. É obrigatória a implementação de mecanismos de segurança baseados em Múltiplo Fator de Autenticação (MFA), para o acesso aos sistemas de gestão dos ambientes de nuvem.

Art. 20º. Conforme previsto na IN PR/GSI nº 5, de 30 de Agosto de 2021, para assegurar a rastreabilidade e o monitoramento de ações no ambiente de nuvem, os logs de acesso ao ambiente devem ser mantidos por:

I - Pelo menos 01 (um) ano, pelo Provedor de Serviços em Nuvem;

II - Pelo menos 05 (cinco) anos, a critério da instituição, em ambiente próprio controlado ou no ambiente do Provedor de Serviços em Nuvem.

Seção VIII

Da proteção de dados

Art. 21º. Dados em repouso ou em trânsito, devem ser trafegados por canais seguros, ou armazenados de maneira a não serem acessíveis sem autorização prévia da instituição, especialmente quando se tratam de dados pessoais, pessoais sensíveis, técnicos ou institucionalmente sensíveis.

Art. 22º. Os mecanismos de segurança devem ser revistos e atualizados regularmente para proteger as informações contra ameaças emergentes.

Seção IX

Da retenção e exclusão de dados

Art. 23º. Os dados devem ser armazenados pelo tempo mínimo necessário para a finalidade estabelecida e, posteriormente, excluídos ou anonimizados.

Art. 24º. Fica proibido o uso de informações da instituição, pelo Provedor de Serviços em Nuvem para propaganda, otimização de mecanismos de inteligência artificial ou qualquer uso secundário não-autorizado.

Art. 25º. Ao término do contrato com o Provedor de Serviços em Nuvem, deve-se garantir a exclusão de todos os dados da organização no ambiente do provedor, com comprovação da exclusão.

Seção X

Da transferência internacional de dados

Art. 26º. Para dados armazenados em nuvens com servidores fora do Brasil, deve-se assegurar a conformidade com as diretrizes da Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), quanto à transferência internacional de dados.

Art. 27º. Dados pessoais ou pessoais sensíveis somente poderão ser hospedados em outros países que possuem legislação compatível com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD).

Art. 28º. Os dados passíveis de serem armazenados e processados em ambientes de nuvem fora do território nacional, devem estar em conformidade com as diretrizes da Política de Segurança da Informação da instituição e com os Art. 17 e Art. 18 da IN PR/GSI nº 5, de 30 de Agosto de 2021.

Seção XI

Do monitoramento e gestão de incidentes

Art. 29º. Devem ser realizados monitoramento e auditorias regulares para avaliar a conformidade com as políticas de segurança e proteção de dados.

Art. 30º. O Provedor de Serviços em Nuvem deve permitir auditorias de segurança da informação e fornecer logs de acesso aos dados armazenados para fins de rastreabilidade.

Art. 31º. O Provedor de Serviços em Nuvem deve dispor de monitoramento contínuo em escala 24x7 (24 horas por dia x 7 dias por semana), para performance, segurança física e lógica do ambiente; e fornecer meios para identificar, avaliar e responder a incidentes de segurança da informação.

Art. 32º. O Provedor de Serviços em Nuvem deve disponibilizar ao menos um meio de contato (Ex: E-mail, Chat, Telefone.) em modelo 24x7 (24 horas por dia x 7 dias por semana), com a instituição.

Art. 33º. O Provedor de Serviços em Nuvem deve fornecer contrato de suporte adicional, ou indicar parceiros certificados para o fornecimento de Suporte Técnico especializado.

Art. 34º. Em caso de incidentes que possam comprometer a segurança dos dados, o provedor de nuvem deverá notificar imediatamente os respectivos agentes internos da instituição, permitindo a adoção de medidas corretivas e mitigadoras.

Art. 35º. Todos os incidentes e violações devem ser documentados e relatados aos agentes responsáveis pela segurança da informação, ao encarregado de proteção de dados (DPO) e à ETIR da instituição.

Seção XII

Das auditorias e avaliações periódicas

Art. 36º. O órgão deve realizar auditorias de segurança e conformidade periodicamente para garantir que o Provedor de Serviços em Nuvem está atendendo aos requisitos de segurança da IN PR/GSI nº 5, de 30 de Agosto de 2021 e das políticas internas da instituição.

Art. 37º. A avaliação deve incluir a verificação de medidas de segurança física, controle de acesso lógico, conformidade com a Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), outros requisitos legais e normas de segurança da informação internacionalmente relevantes.

Seção XIII

Dos termos contratuais e conformidade

Art. 38º. O contrato com o Provedor de Serviços em Nuvem deve incluir cláusulas específicas sobre a segurança da informação, a proteção de dados e o cumprimento das respectivas normas vigentes.

Art. 39º. O Provedor de Serviços em Nuvem deve assinar termos de confidencialidade (NDA) e se comprometer a garantir a proteção dos dados do órgão, proibindo qualquer uso dos dados fora das finalidades estipuladas pela instituição.

RESPONSABILIDADES

Seção I

Do provedor de serviços em nuvem

Art. 40º. Garantir que suas práticas estejam de acordo com as exigências da Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), normativas do governo brasileiro e normas de segurança da informação internacionalmente relevantes, mantendo a segurança e privacidade dos dados.

Art. 41º. Proteger os dados armazenados e em trânsito em conformidade com as exigências de segurança e privacidade estabelecidas na IN PR/GSI nº 5, de 30 de Agosto de 2021.

Art. 42º. Disponibilizar mecanismos para auditorias de conformidade e manter uma comunicação transparente com a instituição em casos de incidentes e manutenções nos sistemas.

Seção II

Do gestor de segurança da informação

Art. 43º. Instituir e coordenar a equipe designada para a elaboração e revisão desta Política de uso de serviços em nuvem.

Art. 44º. Supervisionar a aplicação desta Política de uso de serviços em nuvem.

Art. 45º. Assegurar a contínua efetividade da comunicação com o provedor de serviço de nuvem contratado, de forma a assegurar que os controles e os níveis de serviço acordados sejam cumpridos.

Art. 46º. Supervisionar a aplicação das medidas de correção pelo provedor de serviço de nuvem, em casos de eventuais desvios.

Art. 47º. Comunicar vulnerabilidades e incidentes cibernéticos informados pelo provedor de serviço de nuvem aos órgãos competentes para os seus tratamentos, conforme a relevância das vulnerabilidades e dos incidentes previamente estabelecidos.

Art. 48º. Encaminhar para aprovação da alta administração as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Seção III

Do comitê de governança digital

Art. 49º. Definir os requisitos mínimos de segurança para o trânsito e o armazenamento de dados e informações, custodiados pela instituição, em soluções de computação em nuvem.

Art. 50º. Analisar, em caráter conclusivo, as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem.

Seção IV

Do encarregado de proteção de dados (DPO)

Art. 51º. Supervisionar o cumprimento da Lei nº 13.709, de 14 de Agosto de 2018 (LGPD), no uso de nuvem pública e atuar como ponto de contato para autoridades e titulares de dados.

Seção V

Do departamento de TI

Art. 52º. Avaliar e monitorar o uso de nuvem pública, implementando as medidas técnicas para proteger dados e acessos.

Art. 53º. Revisar periodicamente os provedores de nuvem e realizar auditorias para garantir que estejam em conformidade com as políticas e normativas.

Seção VI

Dos usuários

Art. 54º. Garantir a conformidade com esta política no uso de nuvem pública e relatar qualquer comportamento suspeito ou violação de dados ao departamento de TI via chamado técnico.

Art. 55º. Utilizar, sempre que disponível, recursos adicionais de segurança e múltiplo fator de autenticação (MFA).

Art. 56º. Utilizar os serviços de nuvem em conformidade com as diretrizes de segurança da informação e da Polícia de Segurança da Informação da instituição.

Art. 57º. Reportar qualquer incidente ou anomalia detectada nos sistemas de nuvem ao responsável pela segurança da informação.

Seção VII

Da alta administração do órgão

Art. 58º. Aprovar as minutas de elaboração e de revisões do ato normativo sobre o uso seguro de computação em nuvem e divulgá-las às partes interessadas.

REVISÃO E ATUALIZAÇÃO

Art. 59º. A presente política deve ser revisada a cada 2 (dois) anos, ou sempre que houver alterações na legislação, ou em normativas aplicáveis, para garantir a contínua conformidade e proteção dos dados armazenados em nuvem.

Art. 60º. Esta Norma entra em vigor na data de sua publicação.