MINISTÉRIO DA EDUCAÇÃO

UNIVERSIDADE FEDERAL DO AGRESTE DE PERNAMBUCO

CONSELHO SUPERIOR *PRO TEMPORE*

RESOLUÇÃO CONSUNI Nº 003, DE 02 DE MARÇO DE 2026

Dispõe sobre a Política de Segurança da Informação da Universidade Federal do Agreste de Pernambuco.

O CONSELHO SUPERIOR *PRO TEMPORE* da Universidade Federal do Agreste de Pernambuco (UFAPE), em consonância com a Lei Geral de Proteção de Dados (LGPD) e com as diretrizes e normas estabelecidas pela Secretaria de Governo Digital (SGD) do Ministério da Economia, declara o seguinte:

Art. 1º Fica instituída a Política de Segurança da Informação da UFAPE, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º Esta Política aplica-se a todas as unidades organizacionais da UFAPE, e deverá ser observada por todos os usuários de informação, que são pessoas físicas – servidores ou equiparados, empregados ou prestadores de serviços – habilitadas pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade da UFAPE.

CAPÍTULO I

Disposições Gerais

Art. 3º São objetivos da Política de Segurança da Informação:

I - estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II - estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da confidencialidade, disponibilidade, integridade, confiabilidade e autenticidade das informações;

III - estabelecer competências e responsabilidades quanto à segurança da informação;

IV - nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V - promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da UFAPE;

VI - garantir a conformidade com a legislação e regulamentações aplicáveis em âmbito nacional e internacional;

VII - promover a conscientização e o treinamento de todos os usuários sobre as práticas e os procedimentos de segurança da informação, fomentando uma cultura de segurança na instituição; e

VIII - Assegurar que as ações de segurança da informação sustentem e habilitem o desempenho eficaz e eficiente das atividades de ensino, pesquisa, extensão e administração da UFAPE, garantindo a continuidade dos serviços essenciais.

Art. 4º Para os efeitos desta Resolução e de suas regulamentações, aplicam-se os termos do Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021.

CAPÍTULO II

Dos Princípios e Diretrizes

Art. 5º As ações de segurança da informação da UFAPE são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública Federal, bem como pelos seguintes princípios:

I - disponibilidade, integridade, confidencialidade e autenticidade das informações;

II - continuidade dos processos e serviços essenciais para o funcionamento da UFAPE;

III - economicidade da proteção dos ativos de informação;

IV - respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V - observância da publicidade como preceito geral e do sigilo como exceção;

VI - responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII - alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da UFAPE, assim como demais normas específicas de segurança da informação da Administração Pública Federal;

VIII - conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis; e

IX - educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 6º Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito da UFAPE e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 7º As normas, procedimentos, manuais e metodologias de segurança da informação da UFAPE devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 8º As ações de segurança da informação devem:

I - considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da UFAPE;

II - ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades da UFAPE;

III - ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e

IV - visar à prevenção da ocorrência de incidentes.

Art. 9º O investimento em segurança da informação deve ser dimensionado considerando o valor estratégico do ativo para a missão da UFAPE, a análise de riscos e os potenciais prejuízos à imagem e à continuidade operacional da instituição.

Art. 10. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na UFAPE compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no *caput*, que tramitam pelo ambiente computacional da UFAPE, são passíveis de monitoramento e auditoria pela universidade, respeitados os limites legais.

Art. 11. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação da UFAPE a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da UFAPE.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da UFAPE, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 13. Todos os contratos de prestação de serviços firmados pela UFAPE conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como de suas normas decorrentes.

CAPÍTULO III

Da Gestão de Segurança da Informação

Art. 14. A estrutura de Gestão de Segurança da Informação é composta por:

I - Alta Administração;

II - Comitê de Segurança da Informação, Privacidade e Proteção de Dados;

III - Gestor de Segurança da Informação;

IV - Gestor de Tecnologia da Informação e Comunicação;

V - Encarregado pelo Tratamento de Dados Pessoais;

VI - Responsável Setorial pela Gestão da Integridade;

VII - Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos; e

VIII - Usuários de Informação.

Art. 15 Compete à Alta Administração:

I - fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da UFAPE, bem como para garantir o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

II - formalizar e aprovar a Política de Segurança da Informação da UFAPE, bem como suas alterações e atualizações.

Art. 16 Compete ao Comitê de Segurança da Informação, Privacidade e Proteção de Dados, além das previstas na

portaria que o instituir:

I - assessorar na implementação das ações de segurança da informação;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III - participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV - propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V - deliberar sobre normas internas de segurança da informação; e

VI - avaliar as ações propostas pelo gestor de segurança da informação.

Art. 17 Compete ao Gestor de Segurança da Informação:

I - coordenar o Comitê de Segurança da Informação, Privacidade e Proteção de Dados;

II - coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

III - assessorar a Alta Administração na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

V - promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

VI - incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VII - propor recursos necessários às ações de segurança da informação;

VIII - acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação; e

XI - manter contato direto com o Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à segurança da informação.

Parágrafo único. O Gestor de Segurança da Informação da UFAPE será designado em Portaria da Reitoria e de acordo com a legislação vigente.

Art. 18 Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/ME nº 778, de 4 de abril de 2019, planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 19 Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei Geral de Proteção de Dados (LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

Art. 20 Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 21 Compete à Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

I - facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na UFAPE;

II - monitorar as redes computacionais;

III - detectar e analisar ataques e intrusões;

IV - tratar incidentes de segurança da informação;

V - identificar vulnerabilidades e artefatos maliciosos;

VI - recuperar sistemas de informação;

VII - promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação;

Parágrafo único. A composição, estrutura, recursos e funcionamento da Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos serão definidos em portaria emitida pela Reitoria da UFAPE e de acordo com a legislação vigente.

Art. 22 Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da Universidade Federal do Agreste de Pernambuco (UFAPE).

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 23 A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 24 A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

I - tratamento da informação;

II - segurança física e do ambiente;

III - gestão de incidentes em segurança da informação;

IV - gestão de ativos;

V - gestão do uso dos recursos operacionais e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI - controles de acesso;

VII - gestão de riscos;

VIII - gestão de continuidade;

IX - auditoria e conformidade;

§ 1º O Comitê de Segurança da Informação, Privacidade e Proteção de Dados poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

§ 2º Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

Art. 25 As políticas, normas, procedimentos, orientações ou manuais de que trata o § 2º do art. 24 devem abordar, no mínimo, aspectos relacionados:

I - a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

II - a classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III - a proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV - ao uso aceitável da informação e a utilização de mídias de armazenamento;

V - a entrada e saída de ativos de informação das instalações da organização;

VI - aos perímetros de segurança da organização;

VII - aos controles de acesso baseados no princípio do menor privilégio;

VIII - as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;

IX - aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;

X - ao Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

XI - a Política de Gestão de Ativos da organização, abordando aspectos relacionado:

a) à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para a organização;

b) a manutenção de inventário atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança;

c) uso aceitável de ativos, vedado o uso para fins particulares de seu responsável;

d) o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências;

e) o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; e

f) a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade.

XII - a utilização adequada dos recursos operacionais e de comunicações fornecidos pelo UFAPE, a serem utilizados para fins profissionais, relacionados às atividades da universidade, em conformidade com os princípios éticos e profissionais da instituição, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação da UFAPE;

XIII - aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV - o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV - o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XVI - as políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII - as políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de

acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação da UFAPE;

XVIII - as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando:

a) a análise do ambiente da UFAPE, dos seus ativos de informação e das ameaças à segurança da informação;

b) a adoção de uma metodologia estruturada para identificar riscos, a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência;

c) a avaliação de riscos, de forma a determinar o risco a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; e

d) o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos.

XIX - as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que a UFAPE possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX - as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças;

XXI - as políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

§ 1º As unidades organizacionais da UFAPE devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades da UFAPE, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos na UFAPE devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

CAPÍTULO IV

Das Vedações e Disposições Finais

Art. 26 É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela UFAPE para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 27 São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela UFAPE.

Art. 28 É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 29 É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 30 As unidades organizacionais da UFAPE devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 31 As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através da Ouvidoria da UFAPE.

Art. 32 O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela UFAPE periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 33 A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 34 Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da UFAPE, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 35 Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidos ao Comitê de Segurança da Informação, Privacidade e Proteção de Dados.

APROVADA NA 1a (PRIMEIRA) REUNIÃO EXTRAORDINÁRIA DO CONSELHO SUPERIOR *PRO TEMPORE* DA UNIVERSIDADE FEDERAL DO AGRESTE DE PERNAMBUCO, REALIZADA EM 02 DE MARÇO DE 2026.

PROF. AIRON APARECIDO SILVA DE MELO

- PRESIDENTE -