Ministério da Educação
Universidade Federal do Pampa
Conselho Universitário
Bagé/RS

RESOLUÇÃO CONSUNI/UNIPAMPA Nº 452, DE 28 DE AGOSTO DE 2025

Aprova a Política de Segurança da Informação (PoSIN) da Unipampa.

O CONSELHO UNIVERSITÁRIO da Universidade Federal do Pampa, em sua 124ª Reunião Ordinária, realizada via webconferência no dia 28 de agosto de 2025, no uso das atribuições que lhe são conferidas pelo art. 16 do Estatuto da Universidade, pelo art. 12 da Resolução nº 05, de 17 de junho de 2010 (Regimento Geral) e pelo art. 10 da Resolução nº 308, de 25 de fevereiro de 2021 (Regimento do CONSUNI) e de acordo com o processo nº 23100.009014/2025-22,

RESOLVE:

CAPÍTULO I

DO ESCOPO

Art. 1º Este documento tem como finalidade instituir a Política de Segurança da Informação (PoSIN) no âmbito da Universidade Federal do Pampa (UNIPAMPA), estabelecendo princípios, diretrizes e controles destinados a proteger os ativos de informação da instituição, com o objetivo de assegurar níveis aceitáveis de risco e garantir a confidencialidade, integridade, disponibilidade e autenticidade das informações, inclusive dados pessoais, em conformidade com a Lei geral de Proteção de Dados Pessoais (LGPD) e demais normativos aplicáveis.

Parágrafo único. A PoSIN observa os princípios, objetivos e as diretrizes estabelecidos pelo Governo Federal bem como às disposições constitucionais, legais e regimentais vigentes.

Art. 2º São objetivos específicos 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 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 UNIPAMPA.

CAPÍTULO II

DOS TERMOS E DEFINIÇÕES

Art. 3º Para os efeitos deste documento e das normas por ele originadas, entende-se por:

I - ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação bem como a acessibilidade no uso de ativos de informação de um órgão ou uma entidade;

II - ATIVO DE INFORMAÇÃO: refere-se a qualquer informação ou recurso que tem valor para a organização e deve ser protegido. Esta informação pode estar armazenada em diversos formatos, como documentos, bases de dados, contratos, sistemas de informação e software, e pode envolver também hardware, serviços, pessoas e intangíveis como reputação;

III - AUTENTICIDADE: a propriedade de ser genuíno e passível de verificação. Confiança na validade de uma transmissão, de uma informação ou do emissor da informação;

IV - CONFIABILIDADE: capacidade de um serviço ou sistema de TI de realizar e manter seu funcionamento em circunstâncias de rotina bem como em circunstâncias hostis e inesperadas;

V - CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

VI - DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

VII - DADO PESSOAL SENSÍVEL: 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;

VIII - DETENTOR DA INFORMAÇÃO: pessoa física ou unidade da universidade que detém posse, mesmo que transitória, da informação produzida ou recebida pela UNIPAMPA;

IX - DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

X - INCIDENTE EM SEGURANÇA DA INFORMAÇÃO: qualquer indício de fraude, sabotagem, desvio, falha ou evento indesejado ou inesperado que tenha probabilidade de comprometer as operações do negócio ou ameaçar a segurança da informação;

XI - INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

XII - INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XIII - RECURSO DE INFORMAÇÃO: conjunto de meios utilizados na transferência de documentos, informações, ou dados científicos e técnicos, dos produtores aos usuários desses documentos, informações e dados;

XIV - SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XV - TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

CAPÍTULO III

DISPOSIÇÕES GERAIS

Art. 4º Esta política se aplica a todos os ativos de informação da UNIPAMPA, incluindo dados, sistemas, aplicativos, dispositivos, redes, ambientes computacionais e demais recursos tecnológicos, estejam estes em uso, armazenados ou em trânsito, nos ambientes físicos ou digitais da universidade.

§ 1º A PoSIN abrange todas as unidades e subunidades da UNIPAMPA, bem como servidores, discentes, estagiários, terceirizados, prestadores de serviço, consultores, pesquisadores, visitantes e quaisquer outros que, por qualquer motivo, tenham acesso ou manipulem ativos de informação da universidade.

§ 2º Esta Política também se aplica às interações da UNIPAMPA com outras instituições públicas ou privadas, no que couber, especialmente quando envolverem o tratamento de informações institucionais ou dados pessoais.

CAPÍTULO IV

DOS PRINCÍPIOS E DIRETRIZES

Art. 5º As ações de segurança da informação da UNIPAMPA 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 UNIPAMPA;

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

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

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

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

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

Art. 6º As diretrizes da PoSIN orientam a formulação de políticas específicas, planos e normas complementares no âmbito da UNIPAMPA, visando garantir o atendimento aos princípios estabelecidos nesta política. As diretrizes são definidas a seguir.

Art. 7º As normas, procedimentos, manuais e metodologias de segurança da informação da UNIPAMPA 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 - ser tratadas de forma integrada, respeitando as especificidades das unidades da UNIPAMPA;

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

III - visar à prevenção da ocorrência de incidentes.

Art. 9º O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos à universidade.

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

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional da UNIPAMPA, 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. A assinatura, preferencialmente eletrônica, de Termo de responsabilidade poderá ser exigida como requisito para a concessão de acesso aos recursos de tecnologia da informação da UNIPAMPA. Esse termo formaliza a ciência dos usuários em relação aos princípios desta Política, às responsabilidades decorrentes do uso desses recursos e às penalidades aplicáveis em caso de descumprimento das normas de segurança da informação.

Art. 12. A Política de Segurança da Informação e suas atualizações, bem como normas complementares de segurança da informação da UNIPAMPA, 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 UNIPAMPA conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como suas normas decorrentes.

CAPÍTULO V

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,

III - Gestor de Segurança da Informação;

IV - Gestor de Tecnologia da Informação e Comunicação;

V - Encarregado pelo Tratamento de Dados Pessoais;

VI - Responsável pela Unidade de Controle Interno

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 UNIPAMPA, bem como com 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 UNIPAMPA, bem como suas alterações e atualizações.

Art. 16. Compete ao Comitê de Segurança da Informação – CSI:

I - respaldar a 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 - aprovar e propor alterações à Política de Segurança da Informação e das normas internas de segurança da informação;

IV - deliberar sobre normas internas de segurança da informação;

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

VI - organizar processos de auditorias internas de segurança da informação para assegurar que as áreas estejam em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

Parágrafo único. A composição, estrutura, recursos e funcionamento do Comitê de Segurança da Informação será definido em ato administrativo próprio emitido pela universidade, de acordo com a legislação vigente.

Art. 17. Compete ao Gestor de Segurança da Informação:

I - integrar o Comitê de Segurança da Informação;

II - coordenar a elaboração da Política de Segurança da Informação 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;

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

XII - 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.

Parágrafo único. O Gestor de Segurança da Informação da UNIPAMPA será designado em ato administrativo próprio 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 nº 13.709, de 14 de agosto de 2018 (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 universidade;

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 - atuar na recuperação de sistemas de informação comprometidos por incidentes;

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 ato administrativo próprio emitido pela universidade, de acordo com a legislação vigente.

Art. 22. Compete aos Usuários de Informação conhecer e cumprir esta política, assim como as demais normas específicas de segurança da informação da UNIPAMPA.

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 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 pessoais e a ANPD;

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

XI - a Política para gestão de ativos de informação e serviços deve abordar a proteção, classificação, inventário, uso aceitável, mapeamento de vulnerabilidades, monitoramento e investigação de incidentes de segurança e privacidade.

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

XIII - aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a implantação de soluções tecnológicas contra códigos maliciosos 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 UNIPAMPA;

XVIII - as políticas e procedimentos para a gestão de riscos de segurança da informação na UNIPAMPA devem incluir análise de ambiente, identificação, documentação, avaliação e tratamento de riscos, com priorização para mitigação ou aceitação.

XIX - as políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que a universidade 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 de Gestão de Mudanças para ativos de informação, respaldados por relatórios de risco, devem definir papéis, responsabilidades e processos formais.

XXI - as políticas e procedimentos para auditoria e conformidade devem incluir o Plano de Verificação e o Relatório de Avaliação. O Plano detalha unidades, aspectos, ações, documentos e responsabilidades, enquanto o Relatório especifica ações, parecer e recomendações.

§ 1º As unidades da UNIPAMPA 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 UNIPAMPA 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 universidade 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 VI

DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 26. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela universidade 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 universidade.

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 da UNIPAMPA devem atuar junto ao Gestor de Segurança da Informação para 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 dos seguintes canais:

I - e-mail: abuse@unipampa.edu.br;

II - correspondência oficial (Ofício);

III - Sistema de Gerenciamento de Chamados.

Art. 32. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pelo CSI 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 UNIPAMPA, 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.

Art. 36. As normas referentes à segurança da informação devem estar harmonizadas com as disposições constantes nesta política.

Art. 37. Fica revogada a Resolução CONSUNI/UNIPAMPA nº 284, de 20 de outubro de 2020, que Dispõe sobre a Política de Segurança da Informação e Comunicação no âmbito da Universidade Federal do Pampa.

Art. 38. Esta PoSIN entra em vigor na data de sua publicação.

Bagé, 28 de agosto de 2025.

Edward Frederico Castro Pessano

Presidente do CONSUNI