Universidade Federal do Pampa
Conselho Universitário

RESOLUÇÃO CONSUNI Nº 284, DE 28 DE OUTUBRO DE 2020

Dispõe sobre a Política de Segurança da Informação e Comunicação no âmbito da Universidade Federal do Pampa.

O CONSELHO UNIVERSITÁRIO da Universidade Federal do Pampa, em sua 37ª Reunião Extraordinária, realizada no dia 28 de outubro de 2020, 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), pelo art. 10 da Resolução nº 33, de 29 de setembro de 2011 (Regimento do CONSUNI) e de acordo com o constante no processo nº 23100.018753/2019-67,

RESOLVE:

CAPÍTULO I
DO ESCOPO

Art. 1º A política de segurança da informação e comunicação (POSIC) tem por escopo a instituição de diretrizes estratégicas, com o objetivo de assegurar a integridade dos dados e das informações da Universidade Federal do Pampa (UNIPAMPA) contra ameaças e vulnerabilidades, de modo a preservar os seus ativos, assim como a sua imagem institucional.

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

Art. 2º Esta POSIC tem por objetivo estabelecer mecanismos e controles para garantir a efetiva proteção dos dados e informações produzidos ou custodiados pela universidade, preservando a disponibilidade, integridade, confiabilidade e autenticidade das informações.

Art. 3º Esta política visa a estabelecer os direitos e os deveres a todos que tiverem acesso às informações ou aos recursos de tecnologia da informação e comunicação (TIC) desta instituição, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Art. 4º A POSIC deve ser divulgada a todos os usuários da UNIPAMPA e publicada em sítio institucional, permanecendo disponível para a sociedade.

Parágrafo único. Os procedimentos de segurança da informação e comunicação devem ser divulgados apenas às áreas relacionadas a sua execução.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para os efeitos deste documento e das normas por ele originadas, entende-se por:

I - informação: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

II - ativos de informação: conjunto de dados e informações gerados, armazenados e processados na universidade bem como os locais onde se encontram e as pessoas que têm acesso a eles;

III - 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;

IV - segurança da informação e comunicação (SIC): proteção da informação contra ameaças a fim de garantir a continuidade do negócio, minimizar os riscos e maximizar a eficiência e a efetividade das ações do negócio;

V - detentor da informação: pessoa física ou unidade da universidade que detém posse, mesmo que transitória, da informação produzida ou recebida pela UNIPAMPA;

VI - 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;

VII - 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;

VIII - disponibilidade: propriedade de que a informação esteja acessível e utilizável por pessoa física, sistema, órgão ou entidade;

IX - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizados ou credenciados;

X - integridade: propriedade de que a informação não esteja modificada ou destruída de maneira não autorizada ou acidental;

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

XII - 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; e

XIII - equipe de tratamento e resposta a incidentes em redes computacionais (ETIR): grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

CAPÍTULO III

DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º Este documento tem como referências legais e normativas:

I - Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual de programa de computador, sua comercialização no País e dá providências;

II - Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre a Lei de Acesso à Informação;

III - Decreto nº 7.724, de 16 de maio de 2012, que dispõe sobre o acesso às informações;

IV - Decreto nº 9.637, de 26 de dezembro de 2018, o qual institui a política nacional de segurança da informação;

V - Instrução Normativa GSI/PR nº 1, de 13 de junho de 2008, que disciplina a gestão de segurança da informação e comunicação na Administração Pública Federal, direta e indireta e dá outras providências;

VI - Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 30 de junho de 2009, que estabelece diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da política de segurança da informação e comunicação nos órgãos e entidades da Administração Pública Federal, direta e indireta;

VII - Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, que disciplina a criação da ETIR nos órgãos e entidades da Administração Pública Federal, direta ou indireta;

VIII - Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 11 de novembro de 2009, que disciplina as diretrizes para a gestão de continuidade de negócios nos aspectos relacionados à segurança da informação e comunicação (GCN) nos órgãos e entidades da Administração Pública Federal, direta ou indireta;

IX - Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 19 de agosto de 2010, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas equipes de tratamento e resposta a incidentes em redes computacionais (ETIR) dos órgãos e das entidades da Administração Pública Federal, direta ou indireta;

X - Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 15 de fevereiro de 2013, que estabelece diretrizes para o processo de gestão de riscos de segurança da informação e comunicação (GRSIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta;

XI - Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 15 de julho de 2014, que disciplina as diretrizes para a implementação de controles de acesso relativos à segurança da informação e comunicação nos órgãos e nas entidades da Administração Pública Federal, direta ou indireta;

XII - Norma Complementar nº 21/IN01/DSIC/GSI/PR, de 8 de outubro de 2014, que disciplina o gerenciamento de incidentes de segurança em redes de computadores realizado pelas equipes de tratamento e resposta a incidentes em redes computacionais (ETIR) dos órgãos e entidades da Administração Pública Federal, direta ou indireta;

XIII - Norma ABNT NBR ISO/IEC 27002:2005, que institui o código de melhores práticas para a segurança da informação;

XIV - Norma ABNT NBR ISO/IEC 27001:2006, que provê modelo para estabelecer, implementar, operar, monitorar, analisar criticamente, manter e melhorar um sistema de gestão de segurança da informação;

XV - Norma ABNT NBR ISO/IEC 27005:2008, que institui o código de melhores práticas para a gestão de riscos de segurança da informação; e

XVI - Resolução CONSUNI nº 49, de 27 de setembro de 2012, que disciplina a gestão da propriedade intelectual no âmbito da UNIPAMPA.

CAPÍTULO IV

DOS PRINCÍPIOS

Art. 7º A POSIC deve obedecer aos princípios constitucionais, administrativos e do arcabouço legislativo vigente que regem a Administração Pública Federal, com destaque para:

I - confidencialidade, autenticidade, disponibilidade e integridade, conforme diretrizes de SIC; e

II - alinhamento estratégico, diversidade organizacional, responsabilidade, clareza e transparência.

Art. 8º A SIC é responsabilidade de todos, baseada em hábitos, posturas, responsabilidade e cuidados constantes no momento do uso dos ativos de informação.

Art. 9º Os dirigentes das unidades e demais chefias da UNIPAMPA assumem o compromisso de atuar junto à ETIR naquilo que porventura sejam solicitados e de desenvolver suas atividades de forma colaborativa em estrita observância às orientações determinadas pela ETIR, naquilo que tange à SIC, objetivando minimizar as vulnerabilidades e ameaças que possam comprometer o negócio da instituição.

Art. 10 A utilização dos ativos de informação deve ser sempre compatível com a ética, legalidade e finalidade das atividades desempenhadas pelo usuário.

Art. 11 Toda informação produzida ou armazenada na UNIPAMPA é de sua propriedade, conforme dispõe o art. 7º da Resolução CONSUNI nº 49/2012.

CAPÍTULO V

DAS DIRETRIZES GERAIS

Art. 12 As diretrizes de segurança da informação estabelecidas nesta POSIC aplicam-se aos ativos de informação produzidos, obtidos de terceiros e/ou mantidos no âmbito da UNIPAMPA, assim como a todos os ativos de tecnologia da informação que compõem o seu patrimônio. Essas diretrizes devem ser seguidas por todos os envolvidos, que se tornam responsáveis por sua aplicação.

Seção I

Do Tratamento da Informação

Art. 13 Todo ativo de informação sob a responsabilidade da UNIPAMPA é considerado um bem e será protegido pela instituição de acordo com as diretrizes descritas nesta POSIC e nas demais regulamentações em vigor, com o objetivo de minimizar os riscos aos serviços e às atividades bem como preservar a imagem institucional.

Art. 14 A classificação da informação, no âmbito da UNIPAMPA, obedecerá às diretrizes estabelecidas pela Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação – LAI), e suas regulamentações pelo Governo Federal e pelo Serviço de Informação ao Cidadão.

Seção II

Do Tratamento de Incidentes de Segurança da Informação

Art. 15 Para evitar ou minimizar os impactos de situações de interrupção dos sistemas de informação e comunicação causados por incidentes, a universidade deverá manter um plano de gerenciamento de incidentes, elaborado e alinhado de acordo com o programa de gestão de continuidade de negócios, conforme a legislação vigente.

Art. 16 Os procedimentos para o gerenciamento e tratamento de incidentes de segurança da informação serão fixados em norma específica.

Seção III

Da Gestão de Riscos

Art. 17 A UNIPAMPA deve adotar processo contínuo de GRSIC, conforme a legislação vigente.

Parágrafo único. Os processos de GRSIC serão descritos em norma complementar, de acordo com as diretrizes expostas nesta POSIC.

Seção IV

Da Gestão de Continuidade

Art. 18 Com o objetivo de evitar situações de interrupção e manter em funcionamento seus sistemas de informação e comunicação, a UNIPAMPA, através da DTIC, deverá manter um programa de gestão da continuidade de negócios, conforme a legislação vigente.

Parágrafo único. Os processos de gestão da continuidade de negócios serão descritos em norma complementar, de acordo com as diretrizes expostas nesta POSIC.

Seção V

Da Auditoria e Conformidade

Art. 19 A DTIC, com apoio da sua ETIR, deverá propor normas complementares a fim de manter registros, como mecanismo de auditoria, que possibilite o rastreamento, acompanhamento, controle e a verificação de acesso aos serviços, sistemas de informação e à rede interna, em conformidade com a legislação vigente.

Seção VI

Dos Controles de Acesso

Art. 20 A concessão de acesso aos ativos de informação da UNIPAMPA tem por objetivo garantir aos usuários a realização de suas atividades.

Art. 21 A entrada e a saída de equipamentos e materiais que contenham ou viabilizem o fluxo de informações institucionais da UNIPAMPA serão registradas e autorizadas por autoridade competente mediante procedimento formal.

Art. 22 Os ativos de informação na UNIPAMPA devem ser direcionados por seus usuários para a realização das atividades de ensino, pesquisa, extensão e de administração desempenhadas nos limites da ética, razoabilidade e legalidade.

Art. 23 A conta de acesso e a senha de cada pessoa são únicas, individuais e intransferíveis, sendo reconhecidas como equivalentes a sua assinatura e representam nível de delegação concedida para o desempenho de suas funções.

Art. 24 Os processos e procedimentos que disciplinam o acesso físico e lógico aos ativos de TIC da UNIPAMPA serão descritos em norma complementar, como forma de garantir sua proteção.

Seção VII

Do Uso de E-mail

Art. 25 Os usuários internos da UNIPAMPA terão direito a um endereço pessoal de correio eletrônico, que terá única titularidade, determinando a responsabilidade sobre sua utilização.

Seção VIII

Do Acesso à Internet

Art. 26 O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deverá ser regido por norma interna, atendendo esta POSIC, demais orientações governamentais e a legislação vigente.

CAPÍTULO VI

DAS PENALIDADES

Art. 27 Todos os usuários envolvidos responderão administrativa, civil e/ou penalmente pelo prejuízo que ocasionarem à UNIPAMPA em decorrência do descumprimento das regras previstas nesta POSIC, nas demais normas internas e/ou na legislação vigente.

CAPÍTULO VII

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 28 Esta é a estrutura para a gestão de segurança da informação e comunicação na UNIPAMPA, definida na Resolução CONSUNI nº 83, de 30 de outubro de 2014, e em suas alterações:

I - gestor de segurança da informação e comunicação;

II - Comitê de Segurança da Informação e Comunicação (CSIC); e

III - ETIR.

Art. 29 O Presidente do Comitê de Governança Digital (CGD) deve, conforme definido em Portaria Normativa, atuar como Gestor de segurança da informação e comunicação.

Art. 30 Compete ao gestor de segurança da informação e comunicação:

I - promover a cultura de SIC;

II - acompanhar as investigações e as avaliações dos danos decorrentes de incidentes de segurança;

III - propor recursos necessários às ações de SIC;

IV - coordenar o CSIC e a ETIR;

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na SIC;

VI - manter contato permanente com o Departamento de Segurança da Informação e Comunicação (DSIC) do Gabinete de Segurança Institucional (GSI) da Presidência da República e com o Centro de Atendimento a Incidentes de Segurança (CAIS) da Rede Nacional de Pesquisa (RNP) para o trato de assuntos relativos à SIC;

VII - propor normas relativas à segurança da informação e comunicação;

VIII - promover a melhoria contínua nos processos e controles de SIC; e

IX - desenvolver um plano de conscientização em segurança da informação e comunicação a fim de que todos os servidores da UNIPAMPA tenham ciência do assunto.

Art. 31 O CGD, instituído por Portaria Normativa expedida pelo Reitor da UNIPAMPA, deve:

I - atuar como CSIC;

II - assessorar a implementação das ações de SIC;

III - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SIC;

IV - propor normas e procedimentos internos relativos à SIC, em conformidade com as legislações existentes sobre o tema;

V - propor investimentos e definir a ordem de prioridade de execução dos projetos e a aplicação dos recursos necessários ao cumprimento da POSIC;

VI - monitorar a aplicação dos recursos para a SIC;

VII - propor prioridade em assuntos relacionados à SIC; e

VIII - acolher e analisar as demandas quanto à SIC.

Art. 32 A UNIPAMPA constituirá ETIR e, no seu documento de constituição, adotará as recomendações do Anexo A da Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 14 de agosto de 2009, ou do documento correspondente que venha a substituí-lo.

Parágrafo único. A ETIR será instituída por portaria normativa expedida pelo Reitor.

CAPÍTULO VII

DA ATUALIZAÇÃO

Art. 33 Esta POSIC deverá ser revisada e, se necessário, atualizada a cada 2 anos.

Parágrafo único. A autoridade competente poderá, a qualquer momento, desde que devidamente justificado, propor a revisão da POSIC.

Art. 34 As áreas têm prazo de noventa dias, a contar da publicação desta POSIC, para submeter, à autoridade competente, proposta de atualização ou criação das normas internas complementares e específicas sobre segurança da informação e comunicação.

Art. 35 Esta Resolução entra em vigor em 23 de novembro de 2020.

Bagé, 28 de outubro de 2020.

Roberlaine Ribeiro Jorge

Reitor