UNIVERSIDADE FEDERAL DO OESTE DO PARÁ
CONSELHO SUPERIOR DE ADMINISTRAÇÃO

RESOLUÇÃO CONSAD Nº 102, DE 26 DE SETEMBRO DE 2022

Aprova a Política de Segurança da Informação e Comunicação da Universidade Federal do Oeste do Pará.

A REITORA DA UNIVERSIDADE FEDERAL DO OESTE DO PARÁ, no uso de suas atribuições conferidas pelo Decreto Presidencial de 20 de abril de 2022, publicado no Diário Oficial da União, em 20 de abril de 2022, Edição 75-A, Seção 2, página 1; das atribuições que lhe conferem o Estatuto e o Regimento Geral da Universidade Federal do Oeste do Pará – Ufopa; em conformidade com os autos do Processo nº 23204.007940/2022-52, proveniente do Centro de Tecnologia da Informação e Comunicação – Ctic, e em cumprimento à decisão do egrégio Conselho Superior de Administração – Consad, tomada na 3ª reunião ordinária, realizada em 14 de setembro de 2022, promulga esta resolução.

Art. 1º Fica aprovada a Política de Segurança da Informação e Comunicação – Posic da Universidade Federal do Oeste do Pará.

CAPÍTULO I – DOS OBJETIVOS E DO ESCOPO

Art. 2º A Posic da Ufopa estabelece as diretrizes de segurança da informação a serem observadas no âmbito desta Universidade.

§ 1º A Posic consiste em um conjunto de diretrizes e normas que têm o objetivo de promover a integridade, confiabilidade e confidencialidade das informações geradas, processadas e armazenadas na instituição seja ela em meio físico ou digital.

§ 2º São objetos da política de segurança os ativos de informação primários, ativos de suporte e infraestrutura e ambientes sensíveis.

Art. 3º A Posic deve implementar controles para preservar os interesses dos servidores, estudantes, terceirizados e comunidade em geral contra danos que possam acontecer devido a falhas de segurança da informação.

Art. 4º Para fins de execução desta política são considerados membros da comunidade acadêmica:

I. Discentes;

II. Docentes;

III. Técnicos administrativos em educação;

IV. Servidor em cargo comissionado;

V. Professor visitante e substituto;

VI. Estagiários de outras instituições;

VII. Servidores externos em cooperação técnica com a instituição;

VIII. Funcionários terceirizados;

IX. Quaisquer indivíduos que exerçam alguma atividade administrativa ou acadêmica na Instituição.

Art. 5º A Posic deve ser aplicada a todos os usuários da comunidade acadêmica que tenham acesso aos sistemas, aos computadores, à rede de dados ou aos documentos físicos de propriedade da Ufopa.

Art. 6º A política de segurança deverá conter normas complementares que contemplem a implementação de controles de segurança da informação de maneira estruturada para considerar as necessidades de certos grupos de interesse dentro da organização ou para cobrir tópicos específicos.

Art. 7º A Posic e suas normas complementares devem considerar o que está disposto na Constituição Federal, nos decretos e instruções normativas do Governo Federal.

§ 1º É recomendado que a Posic e suas normas complementares sejam orientadas pelas normas técnicas e boas práticas recomendadas pelos órgãos normativos.

§ 2º Alterações na Constituição Federal, nas leis, decretos e instruções normativas do Governo Federal que afetem diretamente o texto da Posic devem ser corrigidos quando da revisão ou atualização da Posic e sua urgência deve ser analisada pelo Comitê de Governança Digital – CGD.

Art. 8º A Posic passa a vigorar a partir de sua publicação e deve ser atualizada no período máximo de 4 (quatro) anos ou, em prazo mais curto, de acordo com necessidades definidas pelo CGD.

CAPÍTULO II – DAS RESPONSABILIDADES

Art. 9º A Posic deve ser elaborada e mantida pelo CGD ou órgão equivalente na Instituição e aprovada pelo Consad.

Art. 10. Constituem responsabilidades do CGD:

I. instituir comissão para atualizar o texto da Posic dentro do período estipulado no Art. 8º desta política;

II. aprovar as normas complementares à Posic elaboradas pelos setores pertinentes a cada tema;

III. aprovar artefatos da Posic;

IV. definir metodologia para verificação de conformidade da Posic e suas normas complementares;

V. auditar a conformidade da Posic e suas normas complementares nos setores da Ufopa;

VI. divulgar a Posic, seus artefatos e as normas complementares;

VII. elaborar procedimentos para abertura de processo administrativo disciplinar quando da reincidência de infrações da Posic e suas normas complementares.

Art. 11. É dever de todos os usuários de ativos de Tecnologia da Informação – TI da Ufopa:

I. conhecer a Posic e manter níveis de segurança adequados, seguindo as suas diretrizes e normas complementares;

II. adotar comportamento seguro, assumindo atitude pró-ativa e engajada no que diz respeito à proteção das informações da Universidade.

Parágrafo único. A Posic também deverá se aplicar a qualquer usuário externo, com acesso temporário, convidado ou casos excepcionais em que seja concedido acessos a recursos de redes e sistemas institucionais da Ufopa cabendo ao Ctic o cadastro e revogação do acesso destes usuários.

Art. 12. É de responsabilidade da Coordenação de Arquivo ou setor equivalente a elaboração de um manual de classificação da informação, bem como, da sua implementação, orientação e treinamentos.

Art. 13. É dever do Ctic ou setor equivalente manter ativo um sistema gestor de segurança da informação e são responsabilidades deste setor:

I. elaborar campanhas de conscientização e prevenção em segurança da informação;

II. criar e executar plano de capacitações e conscientização em segurança da informação;

III. criar modelos de procedimentos padrões em Segurança da Informação;

IV. criar a manter uma equipe de tratamento e resposta a incidentes com aprovação do CGD;

V. registrar, notificar fragilidades aos envolvidos e às autoridades e responder aos eventos de segurança da informação através da sua equipe de tratamento e resposta a incidentes;

VI. notificar ao CGD, através da equipe de tratamento e resposta a incidentes, casos que violem a legislação vigente para análise e abertura de demais procedimentos pertinentes;

VII. criar e manter um inventário de ativos de segurança da informação.

Art. 14. É de responsabilidade do Ctic e suas coordenações a elaboração e manutenção das seguintes normas complementares:

I. norma complementar para desenvolvimento, manutenção e uso de sistemas institucionais através da direção de sistemas ou setor equivalente;

II. norma complementar de infraestrutura de telecomunicações através de sua

coordenação de redes ou setor equivalente;

III. norma complementar para o uso de recursos de tecnologia da informação e consumerização através da sua coordenação de suporte ou setor equivalente;

IV. norma complementar para a gestão de cópias de segurança das informações mantidas pelo Ctic em meio digital.

Parágrafo único. É de responsabilidade do Ctic ou setor equivalente a elaboração de demais normas complementares inerentes a tecnologia da informação e comunicação.

Art. 15. É dever do CGD instigar os devidos setores ou funções para a elaboração de normas complementares para os seguintes tópicos, mas não restrito a eles:

I. norma complementar para a gestão de pessoas acerca do tema segurança da informação sob a responsabilidade da Pró-Reitoria de Gestão de Pessoas – Progep ou setor equivalente;

II. norma complementar para uso, processamento, armazenamento e divulgação de dados pessoais em posse da Ufopa sob a responsabilidade do encarregado de dados ou pessoa indicada pela reitoria para esta função;

III. norma complementar de segurança física de ambientes sensíveis e preservação de ativos físicos sob a responsabilidade da Coordenação de Segurança Patrimonial ou setor equivalente;

CAPÍTULO III – DO MANUSEIO DAS INFORMAÇÕES INSTITUCIONAIS

Art. 16. É dever do criador da informação classificá-la de acordo com manual de classificação da informação elaborado e aprovado pelo CGD.

Art. 17. Cabe a qualquer indivíduo da comunidade acadêmica proceder de maneira adequada quanto a manipulação de quaisquer informações da Instituição seja em formato físico ou digital, pública ou restrita, em consonância com esta Posic.

Art. 18. Cabe aos pesquisadores zelar pelas informações provenientes de pesquisas científicas, tanto aquelas armazenadas em servidores ou dispositivos da Instituição como as que estiverem em dispositivos particulares dos pesquisadores ou em nuvem externa.

Art. 19. Cabe a qualquer indivíduo da comunidade acadêmica proceder de maneira adequada com as informações em meio digital respeitando os procedimentos para seu armazenamento e compartilhamento com meios de armazenamento externos à Instituição.

Art. 20. Cabe a qualquer indivíduo da comunidade acadêmica proceder de maneira adequada quanto a criação e manipulação de documentos classificados como sigilosos de acordo com o manual de classificação da informação.

Art. 21. Docentes e técnicos devem manipular de maneira adequada as informações de discentes referentes a todo o seu percurso acadêmico dentro da Instituição, sejam em

arquivos físicos ou digitais.

Art. 22. A Instituição deve zelar pela produção acadêmica da Instituição criando mecanismos de segurança para o armazenamento de trabalhos de conclusão de curso, dissertações, teses e artigos elaborados por seus discentes e docentes.

Art. 23. Serão elaborados procedimentos que visem proteger a memória documental da Instituição em meio físico e digital.

Art. 24. Todos os setores da Instituição que armazenem e/ou manipulem dados pessoais, identificáveis ou não, devem proceder de acordo com o que rege a norma específica para o tratamento de dados pessoais e demais legislações vigentes pertinentes ao tema.

Art. 25. Em ambientes de acesso restrito é dever de todos:

I. zelar pelas chaves e credenciais de acesso a ambientes restritos;

II. proceder de maneira adequada com documentos físicos em uso e respeitando os procedimentos para seu armazenamento ou arquivamento.

Art. 26. Os processos de admissão e contratação de servidores efetivos, temporários ou terceirizados deverão atentar para as diretrizes de segurança da informação, constantes em norma complementar específica.

§ 1º Todo aquele que prestar serviço à Instituição deve ter conhecimento desta política, de suas normas complementares e procedimentos padrões de segurança da informação.

§ 2º É de responsabilidade da Progep ou setor equivalente informar, aos setores envolvidos, sobre o desligamento de servidores efetivos para o procedimento de revogação de privilégios e acessos a sistemas institucionais e ambientes físicos da instituição.

§ 3º O setor que proceder com a contratação de funcionários terceirizados deve informar, aos setores envolvidos, sobre o desligamento dos mesmos para o procedimento de revogação de privilégios e acessos a sistemas institucionais e ambientes físicos da Instituição.

CAPÍTULO IV – DA SEGURANÇA DOS ATIVOS E AMBIENTES SENSÍVEIS

Art. 27. O Ctic ou setor equivalente deve manter um inventário de ativos de segurança da informação.

§ 1º Os ativos devem estar definidos em um inventário de ativos de segurança da informação cabendo ao Ctic informar aos proprietários sobre estas responsabilidades.

§ 2º Cabe ao Ctic elaborar os procedimentos para o tratamento dos ativos e que estes sejam desenvolvidos e implementados de acordo com o esquema de classificação da informação adotada pela organização.

§ 3º É de responsabilidade do proprietário do ativo a definição do seu uso aceitável seguindo as diretrizes desta política e suas normas complementares.

§ 4º É dever do proprietário a garantia de devolução dos ativos de segurança da informação que estiverem em posse dos usuários, ou sob sua responsabilidade, ao final de sua utilização.

Art. 28. Os sistemas institucionais e as informações geradas por eles constituem bem intangível da Instituição e devem ser protegidos de maneira adequada através de norma complementar específica.

Art. 29. A Instituição deve prover meios para a manutenção de um enlace de conexão com a internet com qualidade e velocidades adequadas a sua demanda.

Art. 30. Infraestrutura de telecomunicação, incluindo, redes de fibra ótica, cabos metálicos e sem fio e seus equipamentos de conexão constituem ativo de suporte e infraestrutura da Instituição e devem ser protegidos de maneira adequada através de norma específica.

Art. 31. Constituem ambientes sensíveis dentro da Instituição todos os locais onde são processadas ou armazenadas informações consideradas sensíveis por seus proprietários.

§ 1º Os responsáveis por ambientes sensíveis devem informar da necessidade de tratamento especial com itens específicos de segurança e controle de acesso ao ambiente.

§ 2º É dever da Instituição atender às solicitações de tratamento especial para ambientes sensíveis devendo designar o setor responsável para atendimento das demandas de acordo com suas especificidades.

Art. 32. São considerados ambientes sensíveis da Instituição, mas não limitados a estes:

I. ambientes administrativos;

II. laboratórios de pesquisa;

III. guaritas e portarias;

IV. o prédio do Ctic na sede e demais campi, salas de equipamentos de telecomunicação e o Data Center.

Art. 33. A Instituição deve prover meios para a manutenção da infraestrutura de telecomunicações, incluindo, redes de fibra ótica, cabos metálicos e sem fio e seus equipamentos de conexão.

Art. 34. Constituem ativos de informação os recursos humanos da Instituição, incluindo, os professores, técnico-administrativos e funcionários terceirizados.

Art. 35. A Instituição deve manter um sistema de vigilância com infraestrutura adequada, incluindo pessoal especializado e equipamentos.

Art. 36. Constitui requisito fundamental para o bom funcionamento de ativos de TI o fornecimento adequado de energia elétrica e contingências para os ambientes que comportem equipamentos de rede e servidores de aplicações.

Art. 37. Os ativos de TI que armazenem ou processem quaisquer informações institucionais devem receber tratamento adequado quanto ao seu manuseio e

movimentação.

Art. 38. É dever do usuário proceder de maneira segura quanto ao uso de dispositivos de armazenamento para a guarda ou movimentação de documentos de acesso restrito.

Art. 39. Ativos de TI que armazenem ou processem quaisquer informações institucionais, mesmo que sejam de propriedade de seus usuários, devem receber o tratamento adequado quanto ao seu manuseio e movimentação, inclusive fora da Universidade.

Parágrafo único. A consumerização deve ser regida por norma complementar própria.

CAPÍTULO V – DO GERENCIAMENTO DE RISCOS E DA CONTINUIDADE DO NEGÓCIO

Art. 40. Deve haver o gerenciamento de riscos em segurança da informação sob a responsabilidade do Ctic em conjunto com as partes interessadas visando a proteção dos serviços da Ufopa, por meio da eliminação, redução ou transferência dos riscos, conforme seja economicamente e estrategicamente viável.

§ 1º Devem ser incluídos, prioritariamente, no gerenciamento de riscos os ativos de maior valor, conforme inventário de ativos mantido pelo Ctic.

§ 2º Os procedimentos para implantação e gerenciamento de riscos em segurança da informação serão definidos em artefato específico elaborado pela Ctic em conjunto com as partes interessadas e aprovado pelo CGD.

Art. 41. O Plano de Continuidade de Negócio – PCN devem ser elaborados pelo Ctic em conjunto com as partes interessadas devendo cobrir os serviços e processos críticos da Ufopa na possibilidade da ocorrência de desastres naturais, falhas de equipamentos, furto, roubo, falhas humanas e qualquer outro tipo de eventualidade que afetar a segurança das informações institucionais.

§ 1º Os PCNs devem passar por validações periódicas a fim de encontrar falhas que possam vir a ocorrer na elaboração de determinado plano, devendo as falhas serem documentadas e os planos corrigidos.

§ 2º Os PCNs devem ser elaborados com base na análise de riscos e terão a aprovação do CGD.

Art. 42. A responsabilidade pela gerência dos riscos, bem como, da elaboração dos planos de continuidade do negócio será compartilhada entre o CGD, o Ctic e os setores responsáveis pela elaboração das normas complementares.

CAPÍTULO VI – DAS AUDITORIAS, FISCALIZAÇÕES, SANÇÕES E PENALIDADES

Art. 43. Todos os membros da comunidade acadêmica estão sujeitos à auditoria em sua utilização dos recursos de TI e ativos de segurança da informação.

Art. 44. Os testes de conformidade da Posic e suas normas complementares serão realizados anualmente por setor ou função designada pelo CGD que deverão entregar relatório e evolução anual de conformidade.

Art. 45. Os procedimentos de auditoria da Posic serão realizados periodicamente por setor ou função designado pelo CGD para observar o cumprimento das políticas pelos membros da comunidade acadêmica.

Art. 46. Havendo evidência de atividade que infrinja a Posic ou normas complementares poderá o setor responsável pelo ativo restringir o acesso da fonte causadora do problema, devendo o fato ser imediatamente comunicado à equipe de tratamento de incidentes do Ctic, à chefia imediata do usuário e ao CGD que deverá deliberar sobre as providências cabíveis.

§ 1º Quaisquer restrições de acesso ao usuário não devem durar mais do que o necessário para a resolução do problema.

§ 2º Em casos de reincidência, poderá o setor responsável pelo ativo solicitar à equipe de tratamento de incidentes do Ctic a suspensão do acesso por um prazo maior até a deliberação do CGD.

CAPÍTULO VII – DAS DISPOSIÇÕES FINAIS

Art. 47. Esta Resolução entra em vigor em 4 de outubro de 2022, ficando revogada a Resolução Consad nº 4, de 20 de outubro de 2015.

Ato publicado na página dos Conselhos Superiores no Sistema Integrado de Gestão de Recursos Humanos – SIGRH.

ALDENIZE RUELA XAVIER:67350020244

Assinado de forma digital por ALDENIZE RUELA XAVIER:67350020244
Dados: 2022.09.27 11:49:01 -03'00'

ALDENIZE RUELA XAVIER
Presidente do Conselho Superior de Administração

ANEXO I

CONCEITOS E DEFINIÇÕES

Define termos referentes à segurança da informação:

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

II. **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;

III. **CONFIDENCIALIDADE** - propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a órgão ou a entidade não autorizada nem credenciados;

IV. **ATIVO** - qualquer coisa que tenha valor para a organização;

V. **ATIVOS DE INFORMAÇÃO** - os meios de armazenamento, transmissão e processamento da informação, os equipamentos necessários a isso, os sistemas utilizados para tal, os locais onde se encontram esses meios, e também os recursos humanos que a eles têm acesso;

VI. **ATIVOS PRIMÁRIOS -** Processos e atividades do negócio e Informação;

VII. **ATIVOS DE SUPORTE E INFRAESTRUTURA** - ativos de hardware, software, rede, Recursos humanos, Instalações físicas e a estrutura da organização sobre os quais os ativos primários se apoiam;

VIII. **AMBIENTE SENSÍVEL -** Espaço físico que comporte ativos de informações críticas para o funcionamento da instituição;

IX. **SEGURANÇA CIBERNÉTICA** – são ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

Também é conhecida como segurança de tecnologia da Informação;

X. **SEGURANÇA DA INFORMAÇÃO** - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XI. **CONSUMERIZAÇÃO** - Uso de dispositivos pessoais de armazenamento e processamento de informações no ambiente corporativo como celulares, tablets e notebooks.

ANEXO II

REFERÊNCIAS NORMATIVAS

I. Norma ABNT NBR ISO/IEC 27001 - Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação - Requisitos

II. Norma ABNT NBR ISO/IEC 27002 - Tecnologia da Informação - Técnicas de Segurança – Código de Prática para controles de segurança da informação

III. Norma ABNT NBR ISO/IEC 27005 - Tecnologia da informação — Técnicas de segurança — Gestão de riscos de segurança da informação

IV. Manual de Governança em Segurança da Informação - Abrapp - Associação Brasileira das Entidades Fechadas de Previdência Complementar

V. Lei Nº 12.965, DE 23 DE ABRIL DE 2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil

VI. Lei Nº 13.709, DE 14 DE AGOSTO DE 2018 – Lei Geral de Proteção de Dados

VII. Instrução Normativa Nº 01, DE 27 DE MAIO DE 2020 - Dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal.

VIII. Decreto Nº 10.332, de 28 de abril de 2020 - Institui a Estratégia de Governo Digital para o período de 2020 a 2022, no âmbito dos órgãos e das entidades da administração pública federal direta, autárquica e fundacional e dá outras providências.

IX. Decreto Nº 9.637, de 26 de dezembro de 2018 - Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação.

X. Portaria Nº 264, REITORIA de 01 de agosto de 2022 - Atualizar a composição do Comitê de Governança Digital (CGD) no âmbito da Universidade Federal do Oeste do Pará (Ufopa), órgão de natureza deliberativa e de caráter estratégico.

XI. Portaria Nº 189, REITORIA de 30 de julho de 2021, institui o Grupo de Trabalho (GT) para atualização da Política de Segurança da Informação e Comunicação no âmbito da Ufopa (Posic), o qual estará subordinado ao Comitê de Governança Digital (CGD), atualizado pela portaria Nº 220/2021.