RESOLUÇÃO N. 010/2023 - CAD/UENP

Institui a Política de Gestão de Riscos em Tecnologia da Informação (PGR-TI) da UENP.

O Reitor da Universidade Estadual do Norte do Paraná – UENP, Prof. Dr. Fábio Antonio Néia Martini, nomeado pelo decreto nº 11.309, de 06 de junho de 2022, do Governo do Estado do Paraná, no uso de suas atribuições legais e regimentais, considerando a edição do Acórdão nº. 963/2022 com as recomendações do Tribunal de Contas do Estado acerca da necessidade de estabelecer diretrizes, capacitar os gestores e realizar a gestão de riscos; o Memorando Interno 22/2022, do Controle Interno da UENP, com recomendações de medidas para dar fiel cumprimento ao Acórdão 963/2022, no que diz respeito à sistematização de práticas relacionadas à gestão de riscos, aos controles internos e à governança; que a boa governança consiste, entre outros, no gerenciamento de riscos e na definição de mecanismos de controles internos necessários ao monitoramento e à avaliação do sistema, assegurando a eficácia e contribuindo para a melhoria do desempenho dos setores ligados à tecnologia da informação; que a gestão de riscos de TI permite tratar com eficiência as incertezas, seja pelo melhor aproveitamento das oportunidades, seja pela redução da probabilidade ou do impacto de eventos negativos, a fim de melhorar a capacidade de gerar valor e fornecer garantia razoável ao cumprimento dos seus objetivos; as recomendações das melhores práticas e os diversos guias, modelos e ferramentas, estabelecidos pelo Departamento de Privacidade e Segurança da Informação da Secretaria de Governo Digital do Governo Federal, que oferecem recursos técnicos para facilitar a implementação de políticas de riscos, segurança e privacidade, nas instituições; e aprovação do Conselho de Administração - CAD, em reunião realizada no dia 04 de dezembro de 2023,

RESOLVE

Art. 1.º Instituir a Política de Gestão de Riscos de Tecnologia da Informação (PGR-TI), na forma do Anexo I desta Resolução.

Gabinete da Reitoria da UENP em
Jacarezinho, 06 de dezembro de 2023

FABIO ANTONIO NEIA MARTINI:70460841904
Assinado de forma digital por FABIO ANTONIO NEIA MARTINI:70460841904
Dados: 2023.12.07 10:38:49 -03'00'

Prof. Dr. Fábio Antonio Néia Martini
Reitor

ANEXO I

POLÍTICA DE GESTÃO DE RISCOS DE TI
DA UNIVERSIDADE ESTADUAL DO NORTE DO PARANÁ

CAPÍTULO I

DISPOSIÇÕES GERAIS

Art. 1º. A Política de Gestão de Riscos de Tecnologia da Informação (PGR-TI) da Universidade Estadual do Norte do Paraná (UENP) tem por finalidade estabelecer os princípios, diretrizes e responsabilidades a serem observados e seguidos no processo de gestão de riscos que competem ao planejamento e à execução de programas, projetos e processos das unidades de Tecnologia da Informação da UENP.

Art. 2º. Para os efeitos desta Resolução, entende-se por:

I - **Processo**: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

II - **Governança**: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

III - **Objetivo organizacional**: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e na obtenção da visão de futuro da organização;

IV - **Meta**: alvo ou propósito com que se define um objetivo a ser alcançado;

V - **Risco**: possibilidade de ocorrência de um evento que tenha impacto negativo no cumprimento dos objetivos da organização;

VI - **Risco inerente**: risco a que uma organização está naturalmente exposta, sem considerar medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

VII - **Risco residual**: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

VIII - **Gestão de riscos**: arquitetura (princípios, objetivos, estrutura, competências e processo) necessária para se gerenciar riscos eficazmente;

IX - **Gerenciamento de risco**: processo para identificar, avaliar, administrar e controlar potenciais eventos ou situações e fornecer segurança razoável no alcance dos objetivos organizacionais;

X - **Controle**: ação tomada com o propósito de certificar-se de que algo se cumpra de acordo com o que foi planejado, modificando ou corrigindo o desempenho organizacional e individual, caso necessário;

XI - **Controle interno da gestão**: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolos, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

XII - **Medida de controle**: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidos sejam alcançados;

XIII - **Disposição a risco**: nível de risco que uma organização está disposta a aceitar;

XIV - **Evento**: ocorrência(s) ou incidência(s) proveniente(s) do ambiente interno ou externo ou mudança em um conjunto específico de circunstâncias, podendo, inclusive, consistir em alguma coisa não acontecer;

XV - **Oportunidade**: possibilidade de que um evento possa atingir positivamente, um determinado objetivo;

XVI - **Perfil de risco**: descrição do conjunto de riscos definido pelo NTI;

XVII - **Resposta ao risco**: qualquer ação adotada para lidar com risco;

XVIII - **Matriz de risco**: ferramenta em que são registrados os riscos identificados, a avaliação de seus impactos e a probabilidade de ocorrência para os processos, etapas, atividades e objetivos institucionais;

XIX - **Plano de gestão de risco**: esquema que especifica a abordagem, os componentes e os recursos a serem aplicados para a gestão de risco;

XX - **Unidades de TI**: Todos os setores da UENP ligados à Tecnologia da Informação, ou seja, os setores de TI dos *Campi* e o NTI;

XXI - **Gestores de Unidades Administrativas**: Todo servidor (Reitor, Pró-Reitor, Coordenador, Diretor, Chefe, Encarregado) com atribuições administrativas nos limites de suas responsabilidades;

XXII - **Gestor de risco**: Coordenador ou Servidor de TI designado e responsável pela gestão do processo e acompanhamento da execução das atividades relacionadas à gestão dos riscos de TI;

XXIII - **Comitê de Segurança da Informação e Privacidade dos Dados**: Órgão da UENP cujas atribuições são avaliar, supervisionar, prestar orientações, desenvolver, propor e atender demandas relacionadas à Lei Geral de Proteção de Dados (LGPD);

XXIV - **Comitê de Tecnologia da Informação**: Órgão da UENP cujas atribuições são promover, orientar, estabelecer, formular e atender demandas relacionadas ao acesso, utilização, manutenção e controle dos recursos computacionais no âmbito da Universidade;

XXV - **Conselho de Administração (CAD)**: Responsável pela definição de políticas administrativas, financeiras e de pessoal e é composto pelo reitor (presidente); vice-reitor; diretores dos *campi*; pró-reitor de administração e finanças; pró-reitor de recursos humanos; pró-reitor de planejamento e avaliação institucional; além de representante dos alunos, dos servidores técnico-administrativos e dos docentes.

XXVI - **Informação**: Dado ou Conjunto de Dados e conhecimento organizados que possam constituir referência sobre determinado acontecimento.

CAPÍTULO II

DOS PRINCÍPIOS E OBJETIVOS

Art. 3º. A Política de Gestão de Riscos de TI observará aos seguintes princípios:

I - Transparência;

II - Ética;

III - Eficiência;

IV - Integridade;

V - Planejamento;

VI - Interatividade;

VII - Dinamismo;

VIII - Contínua melhoria.

Art. 4º. A Política de Gestão de Riscos de TI tem por objetivos:

I - Mapear e aperfeiçoar os processos e as informações relacionadas a riscos e controles, assegurando que os responsáveis pelas tomadas de decisão, em todos os níveis, tenham informações suficientes para identificar e tratar riscos, otimizando as oportunidades e minimizando a ocorrência de ameaças;

II - Fomentar o alcance dos objetivos da organização, reduzindo os riscos a níveis aceitáveis;

III - Estabelecer a gestão de riscos de forma sistemática, estruturada e oportuna;

IV - Fomentar a transparência e o controle social;

V - Relacionar as informações referentes a riscos e controles de gestão ao Planejamento do NTI.

CAPÍTULO III

DAS DIRETRIZES

Art. 5º. São diretrizes para a gestão de riscos:

I - Norma de avaliação de riscos de segurança e privacidade que acompanha esta resolução;

II - A inclusão da gestão e cultura organizacional da UENP ao processo de Planejamento Estratégico;

III - A adoção de metodologias e ferramentas que possibilitem a obtenção de informações úteis à tomada de decisão para a consecução dos objetivos institucionais e para o gerenciamento e a manutenção dos riscos dentro de padrões definidos pelas instâncias supervisoras;

IV - A efetivação do Processo de Gestão de Riscos a cada gestão administrativa, de acordo com o Plano de Gestão de Riscos elaborado pelo Comitê de Tecnologia da Informação da UENP e aprovado pelo Conselho de Administração (CAD).

CAPÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 6º. São instâncias responsáveis pelo Sistema de Gestão de Riscos de Tecnologia da Informação:

I - O Conselho de Administração (CAD);
II - O Comitê de Tecnologia da Informação;
III - O Comitê de Segurança da Informação e Privacidade dos Dados;
IV - Os Gestores de Unidades Administrativas;
V - Os Gestores de riscos de TI.

§1º. Compete ao Comitê de Tecnologia da Informação definir a Política de Gestão de Riscos de TI e avaliar propostas de mudanças e definir a disposição a riscos de TI e assessorar a alta direção.

§2º. Compete ao CAD aprovar a Política e o Plano de Gestão de Riscos de TI e suas alterações, indicar os gestores de riscos, avaliar e aprovar a priorização dos riscos.

§3º. Compete ao Comitê de Segurança da Informação e Privacidade dos Dados, gerenciar a implementação da Gestão de Riscos de TI e dirimir dúvidas quanto à identificação do gestor de determinado risco no âmbito interno das unidades organizacionais.

§4º. Compete aos gestores de áreas gerenciar os riscos, conforme definidos na Política de Gestão de Riscos de TI, monitorando as operações, a tomada de decisões e comunicando as ações realizadas ao Comitê de Tecnologia da Informação.

§5º. Compete aos Gestores dos Riscos de TI executar as atividades do processo de gestão de riscos sob sua responsabilidade.

CAPÍTULO V

DA OPERACIONALIZAÇÃO

Art. 7º. A operacionalização da gestão de riscos deverá contemplar as seguintes etapas:

I - **Entendimento do contexto**: etapa em que são identificados os objetivos relacionados ao processo organizacional com a realização da identificação, da análise, da avaliação, da priorização e tratamento de riscos, da comunicação, do monitoramento, além da definição de contextos externos e internos a serem levados em consideração ao gerenciar riscos;

II - **Identificação de riscos**: etapa em que são identificados e mapeados os possíveis riscos;

III - **Análise de riscos**: etapa em que são identificadas as possíveis causas e consequências do risco;

IV - **Avaliação de riscos**: etapa em que são estimados os níveis dos riscos identificados;

V - **Priorização de riscos**: etapa em que são definidos quais riscos terão suas respostas priorizadas, levando em consideração os níveis calculados na etapa anterior;

VI - **Definição de respostas aos riscos**: etapa em que são definidas as respostas aos riscos, de forma a adequar seus níveis de consumo estabelecidos para os processos organizacionais, além da escolha das medidas de controle associadas a essas respostas;

VII - **Tratamento do risco**: compreende o planejamento e a realização de ações para modificar o risco;

VIII - **Monitoramento**: compreende o acompanhamento e a verificação do desempenho ou da situação de elementos da gestão de riscos;

IX - **Comunicação**: etapa que ocorre durante todo o processo de Gerenciamento de riscos e é determinada pela integração de todas as entidades envolvidas no processo e pelo monitoramento contínuo da Gestão de Riscos, com vistas a sua melhoria.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

.**Art. 8º.** A Política de Gestão de Riscos de TI será reavaliada e readequada sempre que o Comitê de Tecnologia da Informação recomendar.

Art. 9º. Os casos omissos e as excepcionalidades deverão ser resolvidos pelo Conselho de Administração (CAD).