PGR
PLANO DE GESTÃO DE RISCOS
2025-2026

PRÓ-REITORIA DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - PROTIC

RELAÇÃO DOS DIRIGENTES DA ADMINISTRAÇÃO SUPERIOR

REITORIA

João Paulo Sales Macedo
Reitor

Vicente de Paula Censi Borges
Vice-Reitor

ÓRGÃOS SUPLEMENTARES

Moyses Barbosa da Silva Filho
Prefeito Universitário (PREUNI)

Cátia Regina Furtado da Costa
Coordenadora da Biblioteca Central Professor Cândido Athayde (BCPCA)

Arethusa Dantas Pereira
Diretora da Escola de Aplicação Ministro Reis Velloso (EAMRV)

Maria Patrícia Freitas de Lemos
Chefe do Museu da Vila (MUV)

Josenildo de Souza e Silva
Chefe da Estação de Aquicultura (ESTAQ)

André Riani Costa Perinotto
Chefe Editorial da Editora da UFDPar (EDUFDPar)

PRÓ-REITORIAS

Osmar Gomes de Alencar Júnior
Pró-Reitor de Planejamento (PROPLAN)

Rafael Araújo Sousa Farias
Pró-Reitor de Administração (PRAD)

Aurélio Vinícius Araújo Silva
Pró-Reitor de Gestão de Pessoas (PROGEP)

Eugênia Bridget Gadelha Figueiredo
Pró-Reitora de Ensino de Graduação (PREG)

Jefferson Soares de Oliveira
Pró-Reitor de Pós-Graduação, Pesquisa e Inovação (PROPOPI)

Francisco Jander de Sousa Nogueira
Pró-Reitor de Extensão (PREX)

Gilvana Pessoa de Oliveira
Pró-Reitora de Assuntos Estudantis (PRAE)

Silmar Silva Teixeira
Pró-Reitor de Tecnologia da Informação e Comunicação (PROTIC)

RELAÇÃO DOS DIRIGENTES DA UNIDADE

Silmar Silva Teixeira

Pró-Reitor de Tecnologia da Informação e Comunicação

Eduilson Lívio Neves da Costa Carneiro

Diretor de Sistemas e Infraestrutura de Tecnologia da Informação e Comunicação

Valter Antônio de Lima Cavalcante

Coordenador de Sistemas

Leonardo Costa e Silva

Coordenador de Processos, Projetos e Governança de TIC

Heidi Gracielle Kanitz

Coordenadora da Comunicação Institucional

Everaldo Barbosa da Silva Júnior

Chefe da Divisão de Desenvolvimento e Suporte Avançado

Luiz Carlos Moraes de Brito

Chefe da Divisão de Banco de Dados

Luís Fernando Braúna de Meireles

Coordenador de Infraestrutura e Segurança da Informação

José Eliésio Souza Damasceno

Chefe da Divisão de Datacenter e Segurança da Informação

EQUIPE DE ELABORAÇÃO

Portaria PROTIC N° 03, de 07 de fevereiro de 2025

Leonardo Costa e Silva
Coordenador de Processos, Projetos e Governança de TIC

Silmar Silva Teixeira
Pró-Reitor de Tecnologia da Informação e Comunicação

Eduilson Lívio Neves da Costa Carneiro
Diretor de Sistemas e Infraestrutura de Tecnologia da Informação e Comunicação

Valter Antônio de Lima Cavalcante
Coordenador de Sistemas

Heidi Gracielle Kanitz
Coordenadora da Comunicação Institucional

Luís Fernando Braúna de Meireles
Coordenador de Infraestrutura e Segurança da Informação

LISTA DE SIGLAS

CAIS - Centro de Atendimento a Incidentes de Segurança

CCI - Coordenadoria da Comunicação Institucional

CISI - Coordenadoria de Infraestrutura e Segurança da Informação

CMRV – Campus Ministro Reis Velloso

CPPGTIC - Coordenadoria de Processos, Projetos e Governança de TIC

CS - Coordenadoria de Sistemas

CTIRGov - Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

DBD - Divisão de Banco de Dados

DDSI - Divisão de Datacenter e Segurança da Informação

DSITIC - Diretoria de Sistemas e Infraestrutura de TIC

MEC – Ministério da Educação

PDI – Plano de Desenvolvimento Institucional

PRAD - Pró-Reitoria de Administração

PREUNI - Prefeitura Universitária

PROGEP - Pró-Reitoria de Gestão de Pessoas

PROPLAN - Pró-Reitoria de Planejamento

PROTIC – Pró-reitoria de Tecnologia da Informação e Comunicação

RNP - Rede Nacional de Pesquisa

STI – Superintendência de Tecnologia da Informação

TAE – Técnico-Administrativo em Educação

TI - Tecnologia da Informação

TIC - Tecnologia da Informação e Comunicação

UFDPar – Universidade Federal do Delta do Parnaíba

UFPI – Universidade Federal do Piauí

VPN - Rede Privada Virtual

LISTA DE FIGURAS

LISTA DE QUADROS

SUMÁRIO

1. APRESENTAÇÃO

A Pró-Reitoria de Tecnologia da Informação e Comunicação desempenha papel estratégico e essencial no suporte às operações e no alcance dos objetivos da Universidade Federal do Delta do Parnaíba, promovendo a integração, a eficiência e a segurança de processos organizacionais por intermédio de soluções de tecnologia da informação. Neste sentido, a PROTIC é responsável pela gestão, manutenção e evolução da infraestrutura tecnológica, bem como a implementação de sistemas de informação, atuando como pilar para continuidade das atividades e proteção dos ativos de TIC da UFDPar.

No contexto do presente Plano de Gestão de Riscos, a PROTIC está direcionada a identificar, avaliar e mitigar os riscos associados ao uso de TIC, garantindo a resiliência dos sistemas perante ameaças internas e externas. Sua estrutura organizacional é composta por equipes em áreas como infraestrutura de redes, desenvolvimento de software, segurança da informação, suporte técnico, governança de TIC e comunicação institucional. Essa composição permite uma abordagem abrangente e proativa na gestão de riscos, alinhada às melhores práticas e normativas aplicáveis e frameworks de cibersegurança.

A PROTIC é responsável por gerenciar os ativos tecnológicos, incluindo servidores, banco de dados, aplicações corporativas e dispositivos de conectividade, que sustentam os processos críticos da UFDPar. Além disso, atua na capacitação contínua dos servidores e na sensibilização dos usuários quanto às boas práticas de uso da tecnologia, com foco na prevenção de incidentes como vazamento de dados, interrupções de serviço e ataques cibernéticos. A interação com outras unidades da UFDPar é constante, a fim de assegurar que as soluções de TIC estejam alinhadas às necessidades operacionais e estratégicas da UFDPar, ao mesmo tempo em que mitigam os riscos decorrentes de falhas ou obsolescência tecnológica.

No âmbito da gestão de riscos, a PROTIC adota uma abordagem baseada em três pilares: I - prevenção, por meio da implementação de controles e monitoração contínua dos sistemas; II - detecção, utilizando ferramentas para identificar ameaça em tempo real; e III - resposta, com planos de contingência estruturados para minimizar impactos e restaurar a normalidade das operações no menor tempo possível.

Para assegurar a eficácia desse processo, a PROTIC mantém um ciclo contínuo de avaliação de riscos, que inclui a identificação de vulnerabilidades, a análise de probabilidade e impacto, a proposição de medidas mitigatórias e o monitoramento dos resultados. Este Plano de Gestão de Riscos reflete o compromisso da PROTIC em proteger os ativos da UFDPar, promovendo confiabilidade e continuidade dos serviços de TIC. Desta forma, este documento detalha as diretrizes e ações que serão adotadas para enfrentar os desafios do ambiente tecnológico atual, consolidando uma gestão de riscos eficiente e sustentável.

2. ESTRUTURA ORGANIZACIONAL ADMINISTRATIVA E FÍSICA

A Resolução UFDPar nº 2/2020 estabeleceu a estrutura inicial para implantação da Universidade Federal do Delta do Parnaíba, criada através da Lei nº 13.651, de 11 de abril de 2018, por desmembramento do Campus Ministro Reis Velloso da Universidade Federal do Piauí, definindo como um de seus órgãos suplementares, a Superintendência de Tecnologia da Informação.

A Resolução CONSUNI nº 21/2022, criou, *ad* referendum, a Pró-Reitoria de Tecnologia da Informação e Comunicação, extinguindo a STI, sendo esta decisão ratificada através da Resolução CONSUNI nº 24/2022. Desde então, a PROTIC vem provendo serviços de tecnologia da informação e comunicação para auxiliar a universidade a cumprir suas metas de desenvolvimento do ensino, pesquisa e extensão, sendo esta a sua missão.

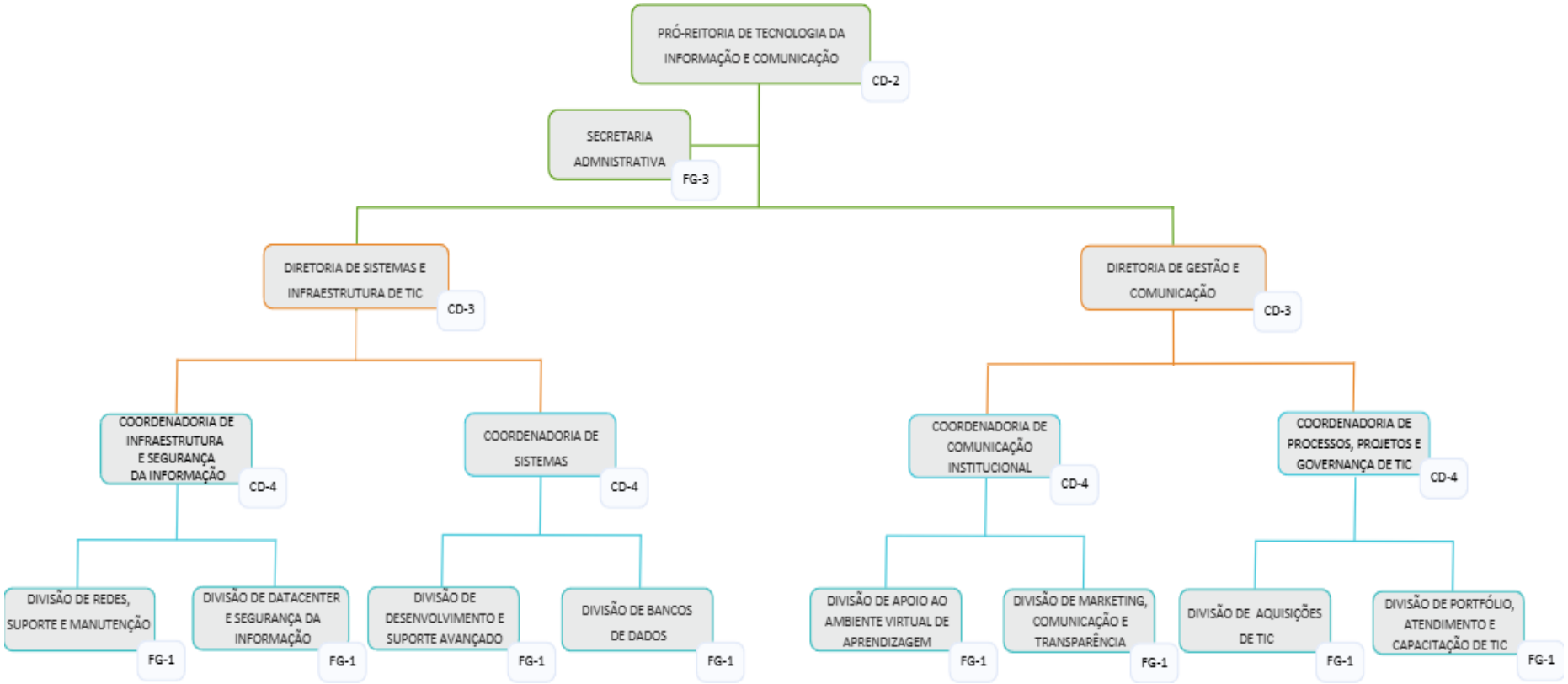
A PROTIC vislumbra para o futuro, ser referência na área de TIC, sendo reconhecida pela excelência nos serviços e suporte tecnológico da UFDPar e executa suas atividades apegada aos seguintes valores:

I. Transparência
II. Conformidade legal
III. Inovação
IV. Integração
V. Trabalho em Equipe
VI. Sistematização
VII. Qualificação

2.1. Organograma da Unidade

A estrutura administrativa da PROTIC está definida na Resolução CONSUNI nº 21, de 22 de setembro de 2022 demonstrada na figura a seguir:

Figura 1: Organograma da PROTIC



2.2. Principais Normas Direcionadores da Unidade

No quadro 1 são apresentadas as bases legais e normas direcionadoras da PROTIC, as quais servem como orientações para o funcionamento e a organização das atividades. A partir delas, a PROTIC estabelece padrões e procedimentos claros, garantindo a uniformidade e a eficiência das ações realizadas.

Quadro 1: Base legal e normas direcionadoras

Referência	Assunto
Constituição Federal/1988	Princípios da Administração Pública
Decreto-Lei nº 200/1967	Organização da Administração Federal
Legislação Aplicada à Contratação de TIC	Leis, Decretos, Instrução Normativa e Portarias referentes a Contratação de TIC
IN SLTI/MPOG nº 1/2010	Compras Sustentáveis
Decreto nº 8.936/2016	Plataforma de Cidadania Digital
IN MP/CGU nº 1/2016	Controles internos, gestão de riscos e governança no âmbito do Poder Executivo Federal
Decreto nº 9.203/2017	Política de Governança da Administração Pública Federal
Decreto nº 9.507/2018	Execução indireta de serviços da Administração Pública Federal
Portaria GM/MPDG nº 443/2018	Serviços preferencialmente objeto de execução indireta
Decreto nº 10.332/2020	Estratégia de Governo Digital para o período de 2020 a 2022
Decreto nº 12.198/2025	Institui a Estratégia Federal de Governo Digital para o período de 2024 a 2027 e a Infraestrutura Nacional de Dados, no âmbito dos órgãos e das entidades da administração pública federal, direta, autárquica e fundacional.
Portaria SGD/ME nº 778/2019	Implantação da Governança de Tecnologia da Informação e Comunicação nos órgãos e entidades pertencentes ao Sistema de Administração dos Recursos de Tecnologia da Informação do Poder Executivo Federal - SISP.
Portaria n°342/2021	Estatuto da UFDPar
Resolução CONSUNI Nº 30/2022	Plano de Transformação Digital
Resolução CONSUNI Nº 37/2023	Altera e acrescenta as competências de cada unidade da PROTIC
Resolução CONSUNI Nº 60/2023	Política e uso do E-mail Institucional

Resolução CONSUNI Nº 63/2024	Política de Segurança da Informação e Comunicação
Resolução CONSUNI Nº 64/2024	Política de Backup e Restauração de Dados
Resolução CONSUNI Nº 68/2024	Política de uso do Site ar
Resolução CONSUNI Nº 69/2024	Política de Gestão de Ativos de Tecnologia da informação e Comunicação
Resolução CONSUNI Nº 75/2024	Plano de Desenvolvimento Institucional UFDPar 2024 - 2028
Resolução CONSUNI N° 82/2024	Política de Gerenciamento de Projetos em Tecnologia da Informação e Comunicação r
Resolução CONSUNI N° 85/2024	Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC)
Resolução CONSUNI Nº 100/2024	Política de Proteção de Dados Pessoais e cria o Comitê Gestor de Proteção de Dados Pessoais
Plano de Desenvolvimento de Unidade 2023 a 2025	Plano de Desenvolvimento de Unidade da PROTIC/UFDPar
Plano de Gestão de Riscos 2023 a 2025	Plano de Gestão de Riscos da PROTIC
Planejamento Estratégico 2023 a 2025	Planejamento Estratégico da PROTIC

Fonte: PROTIC 2025

2.3. Competências das Subunidades e Setores da Unidade

2.3.1. Compete ao Pró-Reitor da PROTIC:

I. Gerenciar e decidir sobre assuntos relacionados à Tecnologia da Informação, assessorando a Alta Administração, orquestrando e contribuindo com a criação de políticas correlatas junto aos Comitês de Governança de TIC e de Segurança da Informação, bem como a sua execução;

II. Planejar e propor soluções para demandas de mudanças legais e administrativas do Governo Federal;

III. Responder às pesquisas, diagnósticos e auditorias do Tribunal de Contas da União (TCU), da Controladoria Geral da União (CGU), da Auditoria Interna da UFDPar e do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Governo Digital, dentre outros, no tocante aos assuntos relacionados à TIC da Instituição;

IV. Promover e publicizar as ações relacionadas à Segurança da informação, Planos de Dados Abertos, Proteção de Dados e outros, bem como a importância Estratégica da TIC para a Instituição, apoiando-se nos Planos e Estratégias de TIC;
V. Construir o planejamento estratégico, tático e operacional que envolvam os processos, projetos e atividades da PROTIC.

2.3.2. Compete à Secretaria Administrativa da PROTIC:

I. Secretariar ao Pró-Reitor da PROTIC, receber, protocolar, encaminhar, triar, registrar e encaminhar documentos e correspondências impressos e eletrônicos;
II. Auxiliar no agendamento dos compromissos, bem como despachar diariamente com o Pró-Reitor da PROTIC;
III. Organizar e secretariar reuniões conduzidas pela Pró-Reitoria;
IV. Confeccionar e organizar documentos, convites e correspondências, realizar atendimentos presenciais e/ou por meio eletrônico, e auxiliar no controle de férias, ausências e processos relacionados aos servidores da PROTIC;
V. Auxiliar no controle patrimonial da PROTIC e na cessão de uso de bens de TIC para outras unidades, bem como prestar apoio ao Pró-Reitor da PROTIC em assuntos diversos;

2.3.3. Compete à Diretoria de Sistemas e Infraestrutura de TIC

I. Assessorar o Pró-Reitor da PROTIC nos assuntos pertinentes às áreas de tecnologia, de desenvolvimento e manutenção de sistemas, de gestão da informação, de segurança da informação, de redes e manutenção de equipamentos;
II. Planejar e priorizar, a médio e longo prazo, em consonância com os projetos desenvolvidos com a Diretoria de Gestão e Comunicação, as atividades relacionadas à implementação e/ou implantação de sistemas; à infraestrutura de TIC, à gestão de recursos do Datacenter, do Parque Computacional e backbone da rede da UFDPar;

III. Implementar projeções, a médio e longo prazo, das mudanças e riscos que envolvem infraestrutura de TIC e sistemas sob a responsabilidade da PROTIC;
IV. Planejar e promover a cultura de desenvolvimento, segurança e operações (DevSecOps) na PROTIC;
V. Promover o uso de melhores práticas, de métodos ágeis (SCRUM, XP, RUP, entre outros), de padrões de projetos, de frameworks e modelos internacionais (COBIT, ITIL, PMBOK, CMMI, ISO 27.001, entre outros) nos processos, projetos e atividades desenvolvidos na Diretoria, Coordenações e Divisões relacionadas àquela;
VI. Planejar e promover a gestão de continuidade dos serviços prestados pela PROTIC, continuous integration/continuous delivery (CI/CD).

2.3.4. Compete à Coordenadoria de Infraestrutura e Segurança da Informação

I. Assessorar o Diretor de Sistemas e Infraestrutura de TIC e ao Pró-Reitor da PROTIC nos assuntos pertinentes às áreas de Tecnologia da Informação e Comunicação;
II. Gerenciar a operacionalização e monitoramento da eficiência dos ativos de TIC; das políticas de Backup, Segurança da Informação, CI/CD;
III. Coordenar as atividades de expansão, modernização, continuidade e manutenção da rede interna, redes sem fio, acesso à internet, virtualização de servidores e equipamentos de redes visando proporcionar a consistência dos serviços computacionais;
IV. Coordenar as ações de apoio/suporte técnico aos usuários;
V. Coordenar a implantação da Política de Segurança da informação e demais políticas que envolvam as atividades da Coordenadoria de Infraestrutura e Segurança da Informação.

2.3.5. Compete à Divisão de Redes, Suporte e Manutenção

I. Gerenciar e executar as atividades relacionadas ao monitoramento dos ativos de TIC sob a responsabilidade da PROTIC, bem como a manutenção no tocante à rede interna, nos níveis e camadas

necessários, conforme os planejamentos realizados pelas unidades competentes da PROTIC;

II. Coordenar e executar as atividades relacionadas ao suporte e manutenção ao usuário tangente ao uso de hardware, acesso à rede, impressoras, instalação de aplicativos, formatação de computadores, e atividades correlatas;

III. Gerenciar e executar ações necessárias para promover a gestão de continuidade dos serviços relacionados com a PROTIC.

2.3.6. Compete à Divisão de Datacenter e Segurança da Informação

I. Promover e executar ações e atividades relacionadas aos planos/políticas de Dados Abertos, Proteção de Dados e Segurança da Informação, em parceria com os respectivos gestores institucionais, sejam eles, unidades, comissões ou comitês;

II. Gerenciar e executar as Políticas de Backup nas bases de dados da instituição, em especial, as gerenciadas pela PROTIC;

III. Gerenciar e executar as atividades de infraestrutura de TIC necessárias às configurações e implantações de novos serviços que dependam do parque tecnológico presente no Datacenter da instituição;

IV. Manter atualizados e seguros os sistemas sob responsabilidade da PROTIC, a fim de minimizar suas falhas de segurança;

V. Buscar implementar as boas práticas em segurança da informação atendendo as normas e guias considerados referências na área;

VI. Implementar nas bases de dados sob a responsabilidade da PROTIC as diretrizes listadas nas normas vigentes, a exemplo da Lei de Acesso à Informação, Lei Geral de Proteção de Dados, dentre outras.

2.3.7. Compete à Coordenadoria de Sistemas

I. Assessorar o Diretor de Sistemas e Infraestrutura de TIC da PROTIC, bem como ao Pró-Reitor, nos assuntos pertinentes ao desenvolvimento, manutenção, implementação, implantação e melhorias em Sistemas

institucionais ou que se relacionem de alguma forma com as atividades da instituição;

II. Coordenar as ações relacionadas a análise, desenvolvimento, testes, implantação, manutenção e demais atividades relativas ao ciclo de vida dos sistemas;

III. Promover ações para a adoção de padrões de projeto de desenvolvimento e manutenção de sistemas, visando qualidade de software;

IV. Planejar e executar as necessidades e condicionantes a serem implementados nas Bases de Dados da PROTIC a fim de atender a legislação vigente;

V. Coordenar a execução das atividades inerentes à Sistemas para a implementação das políticas de segurança da informação (e demais políticas que envolvam o uso de sistemas) seguindo as normas vigentes.

2.3.8. Compete à Divisão de Desenvolvimento e Suporte Avançado

I. Desenvolver e implantar sistemas de informação e comunicação;

II. Gerenciar e executar Análise Negocial e de Requisitos de sistemas a serem implementados, implantados, sustentados e/ou customizados, em sintonia com os planejamentos realizados pelas unidades competentes da PROTIC;

III. Coordenar e executar as atividades de Testes de Software, visando garantir a qualidade dos sistemas institucionais;

IV. Gerenciar e executar as ações necessárias e possíveis para maximizar a segurança dos servidores, da rede e dos sistemas da instituição, em atendimento ao Plano de Segurança da Informação e conformidade com a Política Nacional de Segurança da Informação e as melhores práticas do mercado.

2.3.9. Compete à Divisão de Bancos de Dados

I. Gerenciar e executar em Bancos de Dados os requisitos, condições e recursos a serem implementados, implantados, sustentados e/ou

customizados, em sintonia com a legislação vigente, bem como com os planejamentos realizados pelas unidades competentes da PROTIC;

II. Realizar as modificações nas bases de dados propostas por desenvolvedores da instituição (e/ou de fábricas de software contratadas), gerenciar usuários e perfis de acesso às bases;

III. Monitorar o desempenho, segurança e auditar as atividades;

IV. Implementar a estratégia de Backup e Recovery dos bancos de dados da instituição;

V. Executar em conjunto com a Divisão de Desenvolvimento e Suporte Avançado as políticas de segurança da informação seguindo as normas vigentes.

2.3.10. Compete à Diretoria de Gestão e Comunicação

I. Assessorar ao Pró-Reitor da PROTIC nos assuntos pertinentes às áreas planejamento, governança, gestão, marketing, comunicação e transparência;

II. Planejar e priorizar, a médio e longo prazo, em consonância com os Projetos desenvolvidos com a outra Diretoria da PROTIC, as atividades relacionadas à implementação e/ou implantação de sistemas, gestão de Portfólios de Serviços e aquisições de soluções de TIC;

III. Planejar, a médio e longo prazo, a modernização e integração dos processos de negócio internos à instituição, bem como da Infraestrutura de TIC e Sistemas fazendo uso de TIC;

IV. Planejar o fomento do uso de melhores práticas e frameworks internacionais nos processos, projetos e atividades desenvolvidos na PROTIC;

V. Implementar, coordenar e promover as atividades do Escritório de Projetos e Processos (PPMO);

VI. Coordenar as atividades de capacitação relacionadas ao uso de sistemas, componentes e ferramentas de TIC, em parceria com a Coordenadoria de Comunicação e Conteúdos Digitais, bem como a Pró-Reitoria de Gestão de Pessoas da UFDPar.

2.3.11. Compete à Coordenadoria de Comunicação Institucional

I. Assessorar o Diretor de Gestão e Comunicação ao Pró-Reitor da PROTIC nos assuntos pertinentes às áreas de gestão da comunicação e Relações Públicas;
II. Planejar e Coordenar estratégias e ações prioritárias de Comunicação da UFDPar, de maneira a identificar oportunidades de promoção e eventuais riscos de imagem;
III. Planejar e coordenar políticas, guias e normas que facilitem a organização e a execução das atividades relacionadas com a comunicação institucional;
IV. Gerenciar e controlar a qualidade das imagens, vídeos e produções textuais a serem divulgadas nas redes sociais e portais institucionais gerenciados pela coordenação;
V. Planejar e coordenar as aquisições a serem realizadas para atender as demandas da coordenação.

2.3.12. Compete à Divisão de Apoio ao Ambiente Virtual de Aprendizagem

I. Criação de estratégias de padronização de conteúdos digitais baseados no público-alvo e no potencial de atendimento do material às suas necessidades;
II. Coordenar as atividades de capacitação dos agentes de ensino para o uso das ferramentas e estratégias propostas em parceria/estabelecidas pelas unidades acadêmicas competentes;
III. Monitorar as ações e impactos do uso dos Ambientes Virtuais de Aprendizagem a fim de propor melhorias nas estratégias de ensino.

2.3.13. Compete à Divisão de Marketing, Comunicação e Transparência

I. Coordenar o processo de definição de prioridades de ações de comunicação, marketing e publicidade executadas pela UFDPar;
II. Orientar as ações de publicidade e os eventos executados pela UFDPar;
III. Supervisionar a aplicação de pesquisas de opinião pública e de avaliação de comunicação realizadas pela Universidade;

IV. Buscar junto a reitoria e demais setores da UFDPar, informações relevantes e de interesse público a serem divulgadas à sociedade por meio de ações de publicidade;
V. Planejar e gerenciar campanhas institucionais.

2.3.14. Compete à Coordenadoria de Processos, Projetos e Governança de TIC

I. Assessorar o Diretor de Gestão e Comunicação da PROTIC, bem como ao Pró-Reitor, nos assuntos pertinentes às áreas de Gestão de Projetos, Gestão de Processos e Governança de TIC;
II. Planejar ações que promovam a governança e transparência nos processos, projetos e licitações desenvolvidos na PROTIC;
III. Coordenar a criação e manutenção dos Comitês de Governança temáticos relacionados a TI, bem a gerência de suas reuniões e artefatos gerados;
IV. Realizar os planejamentos anuais relacionados às ações de aquisição, implantação de módulos e/ou sistemas, Planejamentos Estratégicos, Plano Diretor de TIC, Relatório de Gestão (dentre outros) em parceria com as demais Coordenadorias, Diretorias e a Pró-Reitoria;
V. Planejar e gerenciar as ações de aquisição de TIC;
VI. Gerenciar as atividades de Escritório de Projetos e Processos;
VII. Planejar e fazer uso de Data Science, Machine Learning e BI, a fim de promover planos e resultados pautados em níveis técnicos e preditivos.

2.3.15. Compete à Divisão de Aquisições de TIC

I. Planejar e desenvolver artefatos relacionados a aquisições de soluções de TIC, e de soluções onde a PROTIC seja a demandante
II. Atuar em parceria com a Coordenadoria de Compras da instituição de modo a auxiliar os demandantes na consecução das aquisições da instituição;

III. Construir *templates* de projetos que visem a realização, a médio e longo prazo, de aquisições futuras para a PROTIC em conjunto com a Divisão de Portfólio, Atendimento e Capacitação de TIC;
IV. Promover o compartilhamento de conhecimento relacionado com Compras no Setor Público dentre os integrantes da PROTIC;
V. Consolidar as demandas de solução de TIC nos planejamentos de aquisições anuais.

2.3.16. Compete à Divisão de Portfólio, Atendimento e Capacitação de TIC

I. Desenvolver e aprimorar Fluxos de Processo de Negócio em parceria com as unidades organizacionais da instituição, automatizando e indicando adequações aos sistemas e processos existentes;
II. Gerenciar e executar o serviço de atendimento à comunidade da PROTIC;
III. Gerar materiais de apoio à gestão de conhecimento e capacitação dos usuários, através da criação de manuais, relação de respostas às perguntas mais frequentes, e uso de ferramentas de gestão de conhecimento;
IV. Gerar informações que subsidiem sua Coordenadoria na melhoria dos processos e influenciem na e construção dos projetos;
V. Produzir portfólios que contenham projetos relacionados com a PROTIC que facilitem e promovam o planejamento a médio e longo prazo.

Quadro 2: Identificação Institucional da PROTIC

Identificação Institucional	Unidade Organizacional	Composição da Unidade (Resoluções n° 7/2021; 21/2022 e 37/2023 - CONSUNI/UFDPar)							
		Denominação	**Titular**	**Categoria Servidor**	**SIAPE**	**Titulação**	**Portaria**	**Início**	**Término**
Pró-reitoria	Pró-reitoria de Tecnologia da Informação e Comunicação	Pró-reitor	Silmar Silva Teixeira	Docente	1092495	Doutor	614/2023	01/12/2023	31/03/2024
							164/2024	01/04/2024	-
		Secretaria Administrativa da Pró-Reitoria	Não preenchido	-	-	-	-	-	-
Objetivos / Competências		Diretor de Sistemas e Infraestrutura de TIC	Eduilson Lívio Neves da Costa Carneiro	Docente	1287949	Doutor	001/2024	02/01/2024	31/03/2024
							193/2024	01/04/2024	-
Disponível neste Plano de Gestão de Risco, no item 2.2, intitulado: Estrutura Hierárquica da Unidade e Competências		Diretoria de Gestão e Comunicação	Não preenchido	-	-	-	-	-	
		Coordenadoria de Infraestrutura e Segurança da Informação	Luís Fernando Braúna de Meireles	TAE	1199007	Especialização	79/2023	03/02/2023	31/03/2024
							194/2024	26/04/2024	-
		Coordenadoria de Sistemas	Valter Antônio de Lima Cavalcante	TAE	1325432	Especialização	315/2024	03/06/2024	-
		Coordenadoria de Comunicação Institucional	Heidi Gracielle Kanitz	Docente	1864337	Doutor	440/2023	18/07/2023	31/03/2024
							197/2024	01/04/2024	-

	Coordenadoria de Processos, Projetos e Governança de TIC	Leonardo Costa e Silva	TAE	1564965	Especialização	284/2024	18/04/2024	-
	Divisão de Redes, Suporte e Manutenção	Não preenchido	-	-	-	-	-	-
	Divisão de Datacenter e Segurança da Informação	José Eliésio Souza Damasceno	TAE	1127861	Mestrado	389/2024	05/08/2024	-
	Divisão de Desenvolvimento e Suporte Avançado	Everaldo Barbosa da Silva Júnior	TAE	3390230	Especialização	316/2024	03/03/2024	-
	Divisão de Banco de Dados	Luiz Carlos Moraes de Brito	TAE	423529	Especialização	414/2022	10/11/2022	31/03/2024
						196/2024	01/04/2024	-
	Divisão de Apoio ao Ambiente Virtual de Aprendizagem	Não preenchido	-	-	-	-	-	
	Divisão de Marketing, Comunicação e Transparência	Não preenchido	-	-	-	-	-	
	Divisão de Aquisição de TIC	Não preenchido	-	-	-	-	-	
	Divisão de Portfólio, Atendimento e Capacitação de TIC	Não preenchido	-	-	-	-	-	

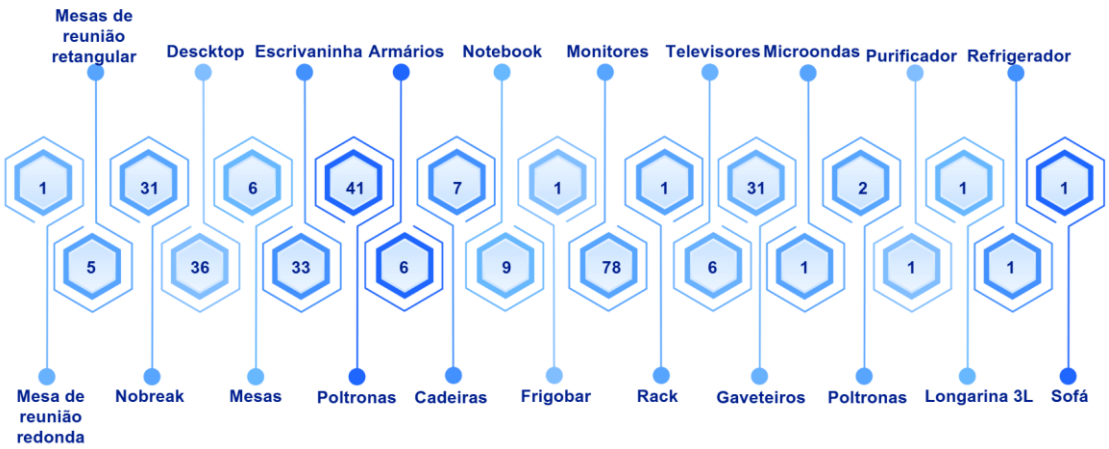
Fonte: PROTIC (2025)

2.4 Estrutura Física

A PROTIC tem seu espaço físico configurado com uma área exclusiva e planejada para atender às crescentes demandas de suas operações. Situada no Campus Ministro Reis Velloso, no setor norte, bloco C, 2º andar, ala leste, a PROTIC tem um espaço que abriga de forma eficiente os equipamentos e materiais de Tecnologia da Informação (TIC), além de proporcionar condições ideais para o desempenho das atividades da equipe. O espaço, estruturalmente estabelecido, é base para futura implementação de um sistema de restrição de acesso às suas dependências, uma medida estratégica que visa reforçar a segurança e a integridade dos recursos tecnológicos, alinhando-se às melhores práticas de gestão e proteção dos ativos da UFDPar.

Complementando essa estrutura, o espaço físico da PROTIC integra instalações críticas para a continuidade e o funcionamento eficiente da UFDPar, como o Data Center e a Sala de Nobreaks, ambos posicionados em locais estratégicos no campus. O Data Center, peça central na arquitetura tecnológica da UFDPar, é local de armazenamento, processamento e gerenciamento de dados sensíveis e essenciais, enquanto a sala de Nobreaks, garante a estabilidade e a continuidade do fornecimento de energia, mesmo em situações adversas. Esses componentes foram alocados em pontos cuidadosamente selecionados, considerando, fatores como segurança física, acessibilidade para manutenção e otimização energética, de modo a assegurar a resiliência e a confiabilidade dos serviços.

Figura 2: Bens da Unidade



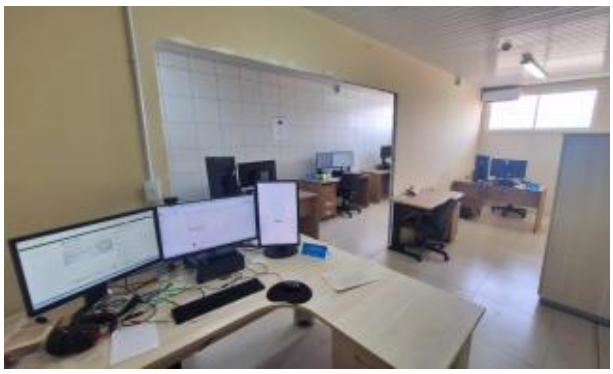
Fonte: PROTIC (2025)

2.3.1. Instalações Físicas do Setor

Figura 3: Gabinete do Pró-reitor

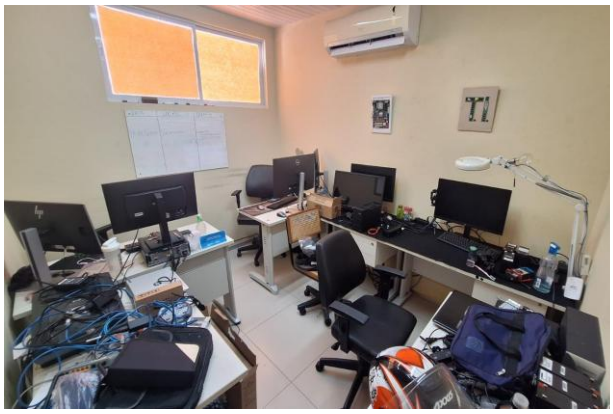
Fonte: PROTIC (2024)

Figura 4: Sala da coordenadoria de Processos, Projetos e Governança de TIC



Fonte: PROTIC (2024)

Figura 5: Sala de Redes, Suporte e Manutenção

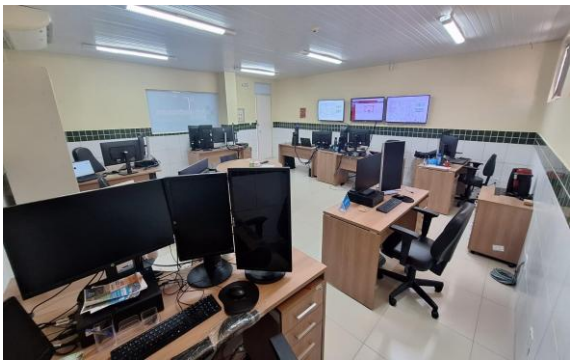


Fonte: PROTIC (2024)

Figura 6: Sala de reuniões

Fonte: PROTIC (2024)

Figura 7: Sala de equipe de infraestrutura, redes e segurança da informação

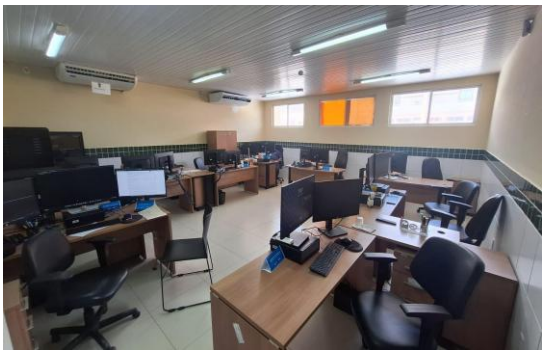


Fonte: PROTIC (2024)

Figura 8: Sala da equipe de Sistemas Integrados

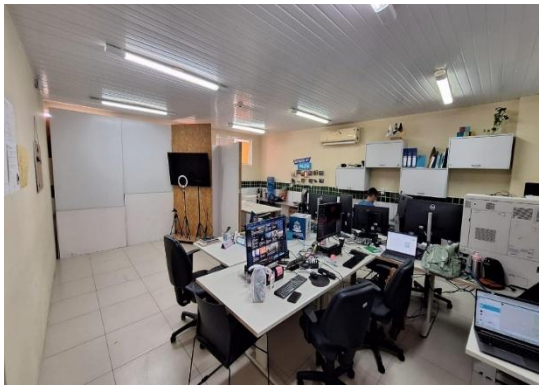
Fonte: PROTIC (2024)

Figura 9: Sala da equipe de Sistemas



Fonte: PROTIC (2025)

Figura 10: Sala da Coordenadoria de Comunicação Institucional



Fonte: PROTIC (2024)

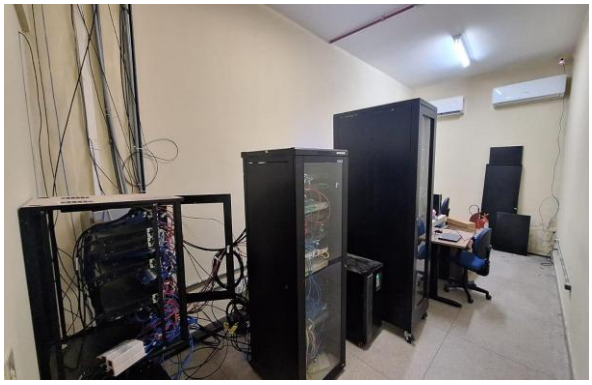
Figura 11: Sala de nobreak e de energia do Data Center

Fonte: PROTIC (2024)

Figura 12: Copa

Fonte: PROTIC (2024)

Figura 13: Sala do Data Center



Fonte: PROTIC (2024)

Figura 14: Depósito

Fonte: PROTIC (2024)

3. OBJETIVOS DA UNIDADE

3.1. Objetivos

Os objetivos da PROTIC funcionam como um norteador, direcionando as ações, recursos e esforços para a concretização de sua visão e missão. Eles representam os resultados esperados que o setor de Tecnologia da Informação e Comunicação busca alcançar em um horizonte temporal claramente estabelecido, refletindo um planejamento estratégico bem estruturado. Esses objetivos não surgem isoladamente; são cuidadosamente alinhados à visão, à missão e aos valores fundamentais da UFDPar, ao considerar uma análise abrangente do ambiente interno, tais como capacidades, recursos e limitações; além do ambiente externo, incluindo tendências tecnológicas, demandas do contexto e expectativas dos usuários. Dessa forma, os objetivos de TIC da PROTIC se integram harmoniosamente aos objetivos estratégicos mais amplos da UFDPar, estabelecendo uma conexão direta entre as iniciativas tecnológicas e as prioridades institucionais.

Quadro 3: Objetivos da PROTIC

INDENTIFICADOR	OBJETIVOS DA UNIDADE	OBJETIVOS INSTITUCIONAIS (PDI)	METAS DO PEI
OU1	Promover a Transformação Digital e Sustentável na UFDPar.	OBJ4, OBJ5, OBJ6, OBJ7 e OBJ10	M43
OU2	Fortalecer a Sustentabilidade na Gestão de TIC.	OBJ7	M102
OU3	Modernizar e garantir a Infraestrutura Tecnológica, a Conectividade e a Segurança de Rede.	OBJ7, OBJ10	M66
OU4	Incentivar a Cultura de Segurança e Conscientização Digital.	OBJ7	M105
OU5	Aprimorar a Comunicação e a Transparência Institucional.	OBJ7 e OBJ10	M45, M47, M66 e M105
OU6	Garantir a Segurança e Governança da Infraestrutura de TI.	OBJ7 e OBJ10	M62, M67 e M68

OU7	Desenvolver, Implementar, Automatizar e Melhorar Processos e Sistemas Digitais.	OBJ7 e OBJ10	M44, M46, M69, M70, M102 e M105
OU8	Gerenciar Estrategicamente e Otimizar Recursos.	OBJ10	M105
OU9	Capacitar e Desenvolver a Equipe.	OBJ10	M51

Nota - OU: Objetivo da Unidade, OBJ; Objetivo Institucional do Plano de Desenvolvimento Institucional (PDI), M: Metas do Planejamento Estratégico (PE)

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

4. ESTRATÉGIA E DESEMPENHO DA UNIDADE

4.1 DIAGNÓSTICO DA UNIDADE

4.1.1. Análise da Matriz SWOT

Para o diagnóstico da PROTIC foi realizada a identificação de riscos, onde foram mapeados os eventos que podem afetar os sistemas de TIC, como falhas de segurança, ataques cibernéticos ou até mesmo falhas em hardware e software. Para este processo, foi realizada a matriz SWOT (forças, fraquezas, oportunidades e ameaças), que permitiu identificar tanto os riscos internos quanto os externos que podem impactar a infraestrutura tecnológica. A análise desses riscos, na qual cada risco foi identificado, foi avaliado com base na sua probabilidade de ocorrência e no impacto potencial, priorizando aqueles que exigem maior atenção. Em seguida, foram avaliados os riscos, comparando-os com os critérios de aceitação da UFDPar, permitindo determinar quais são mais críticos e precisam de tratamento imediato.

Em continuidade, foi incluído o tratamento de riscos, para definir o plano de ação para mitigar, transferir, aceitar ou evitar os riscos e desta forma, passamos ao monitoramento e revisão, a fim de garantir que o risco seja acompanhado de forma contínua, revisando o plano conforme novas ameaças ou mudanças no ambiente de TIC. Após, avançamos na etapa de comunicação e consulta, para garantir que todas as partes envolvidas estejam cientes dos riscos, ações tomadas e alinhadas quanto aos procedimentos de resposta. Por fim, a etapa de documentação, que envolveu o registro de todas as decisões, ações e resultados, facilitando futuras auditorias e possibilitando melhorias contínuas no processo de gestão de riscos.

Quadro 4: Matriz SWOT PROTIC

Forças (Strengths)	Fraquezas (Weaknesses)
➢ Equipe multidisciplinar, engajada, atuando em harmonia e altamente colaborativa; ➢ Servidores qualificados e com conhecimento detalhado dos processos internos; ➢ Quadro funcional em permanente capacitação, com ênfase nos frameworks mais relevantes de segurança e boas práticas em governança; ➢ Desenvolvimento próprio de sistemas e controle da infraestrutura; ➢ Proximidade com os usuários internos ➢ Existência de fluxos e manuais de comunicação, além de programas de divulgação científica e institucional.	➢ Disponibilidade orçamentária limitada; ➢ Morosidade e ineficiência nos processos internos; ➢ Dependência de sistemas sob tutela da Universidade Federal do Piauí; ➢ Obsolescência tecnológica e infraestrutura desatualizada; ➢ Dificuldade na integração de sistemas; ➢ Falta de automação completa; ➢ Gestão de contratos aquém do ideal; ➢ Falta de instrumentos de mensuração de impacto; ➢ Dificuldade em atrair e reter talentos; ➢ Rotatividade de bolsistas e poucos servidores especializados na área de Comunicação. ➢ Resistência à mudança; ➢ Inadequação do espaço físico;
Oportunidades (Opportunities)	**Ameaças (Threats)**
➢ Parcerias estratégicas com outras instituições e imprensa local; ➢ Demanda crescente por Transformação Digital; ➢ Adoção de novas tecnologias; ➢ Modernização da legislação e padrões de conformidade; ➢ Ampliação da comunicação e transparência; ➢ Capacitação continuada; ➢ Abertura do mercado para produtos desenvolvidos no setor; ➢ Ser referência em desenvolvimentos para ensino, pesquisa, extensão e gestão educacional.	➢ Ameaças cibernéticas; ➢ Falta de investimento em TIC; ➢ Obsolescência tecnológica; ➢ Mudanças regulatórias e exigências de conformidade; ➢ Perfis e canais que publicam Fake News; ➢ Alta demanda de desenvolvimento de software. ➢ Volume excessivo de chamados na Central de Serviços; ➢ Desastres naturais; ➢ Furto/Roubo de equipamentos; ➢ Quebra da integridade dos arquivos do banco de dados; ➢ Falha na entrega do serviço em nuvem.

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

4.1.1.1. Pontos Fortes

I. Equipe multidisciplinar, engajada, atuando em harmonia e altamente colaborativa.

Ativo de TIC: Capital Humano – A presença de equipe qualificada e colaborativa, fundamental na identificação, avaliação e mitigação de riscos. Profissionais especializados podem lidar com as ameaças de forma eficaz e rápida, utilizando seu conhecimento para implementar soluções de segurança e melhorar a infraestrutura tecnológica da UFDPar.

II. Servidores qualificados e com conhecimento detalhado dos processos internos

Ativo de TIC: Conhecimento Técnico Interno – O conhecimento profundo dos processos internos garante que a equipe de TIC possa tomar decisões mais seguras sobre como proteger e otimizar os sistemas da UFDPar, aumentando a resiliência da infraestrutura contra ameaças e falhas.

III. Capacitação contínua, com ênfase nos *frameworks* mais relevantes de segurança e boas práticas em governança

Ativo de TIC: Plataformas de Treinamento e Certificação – A capacitação contínua tem permitido que a equipe de TIC se mantenha atualizada sobre as últimas tendências e práticas de segurança. Isso garante que a UFDPar esteja bem equipada para enfrentar os riscos emergentes.

IV. Desenvolvimento próprio de sistemas e controle da infraestrutura

Ativo de TIC: Sistemas e Infraestrutura Interna – O controle interno sobre o desenvolvimento e manutenção dos sistemas permite personalização, maior flexibilidade e segurança. A UFDPar tem implementado as melhores práticas de governança e segurança, sem depender de fornecedores externos que poderiam introduzir riscos adicionais.

V. Proximidade com os usuários internos

Ativo de TIC: *Feedback* dos Usuários e Dados de Uso – A proximidade com os usuários internos possibilita coletar *feedback* para melhorias de sistemas e identificar riscos operacionais. O entendimento das necessidades dos usuários pode ajudar a antecipar problemas antes que se tornem críticos.

VI. Existência de fluxos e manuais de comunicação, além de programas de divulgação científica e institucional

Ativo de TIC: Ferramentas de Comunicação e Colaboração – A existência de sistemas bem definidos de comunicação, como plataformas colaborativas, facilitando a disseminação de informações críticas sobre segurança e processos de gestão de riscos.

4.1.1.2. Pontos Fracos

I - Disponibilidade orçamentária limitada

Ativo de TIC: Orçamento para Atualizações e Investimentos em TIC – A limitação de recursos financeiros pode impedir a atualização ou expansão da infraestrutura de TIC, tornando os sistemas vulneráveis a riscos, como ataques cibernéticos ou falhas de desempenho. Sem um orçamento adequado, a capacidade de implementar melhorias necessárias é reduzida.

II - Morosidade e ineficiência nos processos internos

Ativo de TIC: Sistemas e Processos Internos – A falta de agilidade nos processos pode prejudicar a capacidade de resposta a incidentes de segurança, como a correção de vulnerabilidades. Processos ineficientes tornam a UFDPar mais suscetível a erros e atrasos, impactando a eficácia da gestão de riscos.

III - Dependência de sistemas sob tutela da UFPI

Ativo de TIC: Infraestrutura e Sistemas de Terceiros – A dependência de sistemas ou serviços oferecidos por outras instituições pode representar um risco se essas plataformas falharem ou forem comprometidas. Isso limita o controle da UFDPar sobre a segurança e a continuidade dos serviços.

IV - Obsolescência tecnológica e infraestrutura desatualizada

Ativo de TIC: Equipamentos e Sistemas Tecnológicos – A obsolescência tecnológica pode comprometer a segurança e o desempenho dos sistemas, expondo a UFDPar a falhas e ataques. Equipamentos antigos e desatualizados não possuem a mesma proteção contra ameaças cibernéticas, tornando-os vulneráveis a invasões.

V - Dificuldade na integração de sistemas

Ativo de TIC: Sistemas Desconectados e Interfaces – A falta de integração eficiente entre os sistemas pode criar falhas de comunicação e dificultar a detecção

de riscos em tempo real. Sistemas fragmentados aumentam a complexidade na gestão de dados e podem resultar em vulnerabilidades de segurança.

VI - Falta de automação completa

Ativo de TIC: Processos Automatizados de TI – A falta de automação em áreas-chave da operação de TIC pode aumentar o risco de erro humano e reduzir a capacidade de resposta a incidentes críticos. A automação permite uma gestão mais eficiente de riscos e facilita a realização de tarefas repetitivas sem falhas.

VII - Gestão de contratos aquém do ideal

Ativo de TIC: Contratos e Parcerias de Fornecedores de TIC – A falta de uma gestão de contratos bem estruturada pode resultar em serviços de qualidade inferior, falhas no cumprimento de acordos e aumento dos riscos operacionais.

VIII - Falta de instrumentos de mensuração de impacto

Ativo de TIC: Ferramentas de Monitoramento e Análise de Impacto – A ausência de métricas claras dificulta a avaliação da eficácia das ações de gestão de riscos, dificultando priorizar os problemas mais críticos. Isso também dificulta a identificação de áreas de melhoria e o ajuste da estratégia de segurança.

IX - Dificuldade em atrair e reter talentos

Ativo de TIC: Recursos Humanos Especializados – A falta de profissionais especializados em TIC compromete a capacidade da UFDPar de enfrentar desafios tecnológicos e de segurança. A rotatividade ou a escassez de talentos pode levar a uma diminuição na eficácia da gestão de riscos.

X - Rotatividade de bolsistas e escassez de servidores especializados em Comunicação

Ativo de TIC: Profissionais de Comunicação e TIC – A falta de continuidade na equipe de comunicação, juntamente com a escassez de especialistas em áreas-chave, pode prejudicar a transmissão de informações críticas de segurança para os stakeholders, impactando a eficácia dos planos de resposta a incidentes, além de comprometer a imagem da UFDPar

XI - Resistência à mudança

Ativo de TIC: Cultura Organizacional – A resistência a mudanças tecnológicas ou processos inovadores pode retardar a adoção de novas soluções de segurança, ou impedir a implementação de melhores práticas de governança.

XII - Inadequação do espaço físico

Ativo de TIC: Infraestrutura Física – A inadequação do espaço físico para suportar a infraestrutura de TIC pode aumentar os riscos de falhas operacionais e de segurança, como a falta de ventilação, incêndios ou falhas nos sistemas de energia.

4.1.1.3. Oportunidades

I - Parcerias estratégicas com outras instituições e imprensa local

Ativo de TIC: Alianças e Acordos com Fornecedores e Parceiros – Parcerias com outras instituições, startups e empresas privadas podem proporcionar acesso a novos recursos tecnológicos e colaborar para a melhoria das capacidades de gestão de riscos. Ampliar a relação com a imprensa loca,l ajuda a aumentar a visibilidade de boas práticas de segurança e governança.

II - Demanda crescente por Transformação Digital

Ativo de TIC: Tecnologias Emergentes – O aumento da demanda por transformação digital oferece à UFDPar a chance de adotar novas tecnologias que melhoram a segurança, a eficiência operacional e a gestão de riscos. A transformação digital também oferece a oportunidade de modernizar a infraestrutura tecnológica e integrar novas soluções mais seguras.

III - Adoção de novas tecnologias

Ativo de TIC: Inovações em TI – A implementação de tecnologias emergentes, como inteligência artificial, computação em nuvem e blockchain, pode melhorar a gestão de riscos e oferecer novas oportunidades para fortalecer a segurança dos sistemas, além de otimizar os processos internos.

IV - Modernização da legislação e padrões de conformidade

Ativo de TIC: Ferramentas de Conformidade e Governança – A adaptação a novos regulamentos e padrões de conformidade é uma oportunidade para a UFDPar aprimorar suas práticas de segurança. A implementação de sistemas de conformidade atualizados pode melhorar a resiliência da UFDPar a riscos jurídicos e cibernéticos.

V - Ampliação da comunicação e transparência

Ativo de TIC: Sistemas de Comunicação e Transparência – A melhoria na comunicação interna e externa pode aumentar a eficácia na disseminação de informações críticas sobre segurança e riscos. Transparência nas operações também fortalece a confiança dos *stakeholders* e melhora a imagem institucional.

VI - Capacitação contínua

Ativo de TIC: Plataformas de Treinamento – A capacitação contínua oferece a oportunidade de manter a equipe de TIC bem treinada e preparada para lidar com novas ameaças e desafios, melhorando a gestão de riscos.

VII - Abertura do mercado para produtos desenvolvidos no setor

Ativo de TIC: Soluções Desenvolvidas Internamente – O mercado crescente para produtos e soluções desenvolvidas internamente no setor de TIC abre novas oportunidades de receita e crescimento. Isso pode permitir à UFDPar expandir suas ofertas e se tornar um líder de mercado na criação de soluções tecnológicas inovadoras.

VIII - Ser referência em desenvolvimentos para ensino, pesquisa, extensão e gestão educacional

Ativo de TIC: Sistemas de Ensino e Pesquisa – Tornar-se referência em TIC voltada para o ensino e gestão educacional é uma oportunidade para ampliar a influência da UFDPar no setor, atrair mais colaborações e investimentos, além de melhorar a eficácia dos sistemas educacionais e administrativos, criando um ambiente seguro e inovador.

4.1.1.4. Ameaças

I - Cibernéticas

Ativo de TIC: Sistemas de Defesa Cibernética – A constante evolução das ameaças cibernéticas pode comprometer a segurança dos sistemas de TIC e dados sensíveis. O aumento de ataques como ransomware, phishing e invasões direcionadas torna necessário manter uma estratégia defensiva robusta e em constante atualização.

II - Falta de investimento em TI

Ativo de TIC: Orçamento para Atualizações de TIC – A falta de investimentos adequados pode resultar em sistemas desatualizados e vulneráveis, o que aumenta o risco de falhas operacionais e ataques cibernéticos.

III - Obsolescência tecnológica

Ativo de TIC: Equipamentos e Sistemas Desatualizados – A obsolescência tecnológica é uma ameaça constante, pois sistemas antigos ficam mais vulneráveis a falhas e ataques. A falta de atualização pode comprometer a eficácia das soluções de segurança.

IV - Mudanças regulatórias e exigências de conformidade

Ativo de TIC: Ferramentas de Conformidade – Mudanças repentinas nas regulamentações podem criar desafios para garantir que os sistemas de TIC da UFDPar estejam sempre em conformidade. Falhas na adaptação podem resultar em multas ou danos à reputação.

VI - Perfis e canais que publicam Fake News

Ativo de TIC: Sistemas de Monitoramento de Mídias Sociais – A disseminação de informações falsas pode afetar negativamente a imagem e a reputação da UFDPar. Sistemas de monitoramento e resposta a crises são essenciais para combater fake news.

VII - Alta demanda de desenvolvimento de software

Ativo de TIC: Recursos de Desenvolvimento – O aumento da demanda por novos desenvolvimentos pode sobrecarregar a equipe de TIC, dificultando a entrega de soluções seguras e bem testadas. Isso pode aumentar a probabilidade de falhas de segurança nos sistemas.

VIII - Volume excessivo de chamados na Central de Serviços

Ativo de TIC: Sistema de Suporte e Atendimento – Um volume elevado de chamados pode sobrecarregar os recursos da central de serviços e dificultar a resolução de incidentes críticos, resultando em um impacto negativo na continuidade dos serviços de TIC.

IX - Desastres naturais

Ativo de TIC: Planos de Recuperação e Backups – Desastres naturais podem destruir a infraestrutura de TIC. A ausência de *backups* adequados e planos de recuperação coloca os dados e a continuidade do negócio em risco.

X - Furto/Roubo de equipamentos

Ativo de TIC: Segurança Física e Equipamentos Críticos – O furto de equipamentos tecnológicos pode comprometer dados sensíveis e interromper a operação de sistemas importantes. Medidas de segurança física, como controle de acesso e monitoramento de câmeras, são essenciais para proteger os ativos tecnológicos.

XI - Quebra da integridade dos arquivos do banco de dados

Ativo de TIC: Gerenciamento de Banco de Dados – A quebra da integridade dos dados pode resultar em falhas operacionais graves e comprometimento das

informações críticas. Sistemas de *backup* e integridade de dados são fundamentais para minimizar esse risco.

XII - Falha na entrega do serviço em nuvem

Ativo de TIC: Soluções de Computação em Nuvem – A dependência de serviços em nuvem implica o risco de falhas na entrega do serviço, interrupções ou perda de dados. Garantir a redundância e a segurança na nuvem é vital para evitar impactos negativos no negócio.

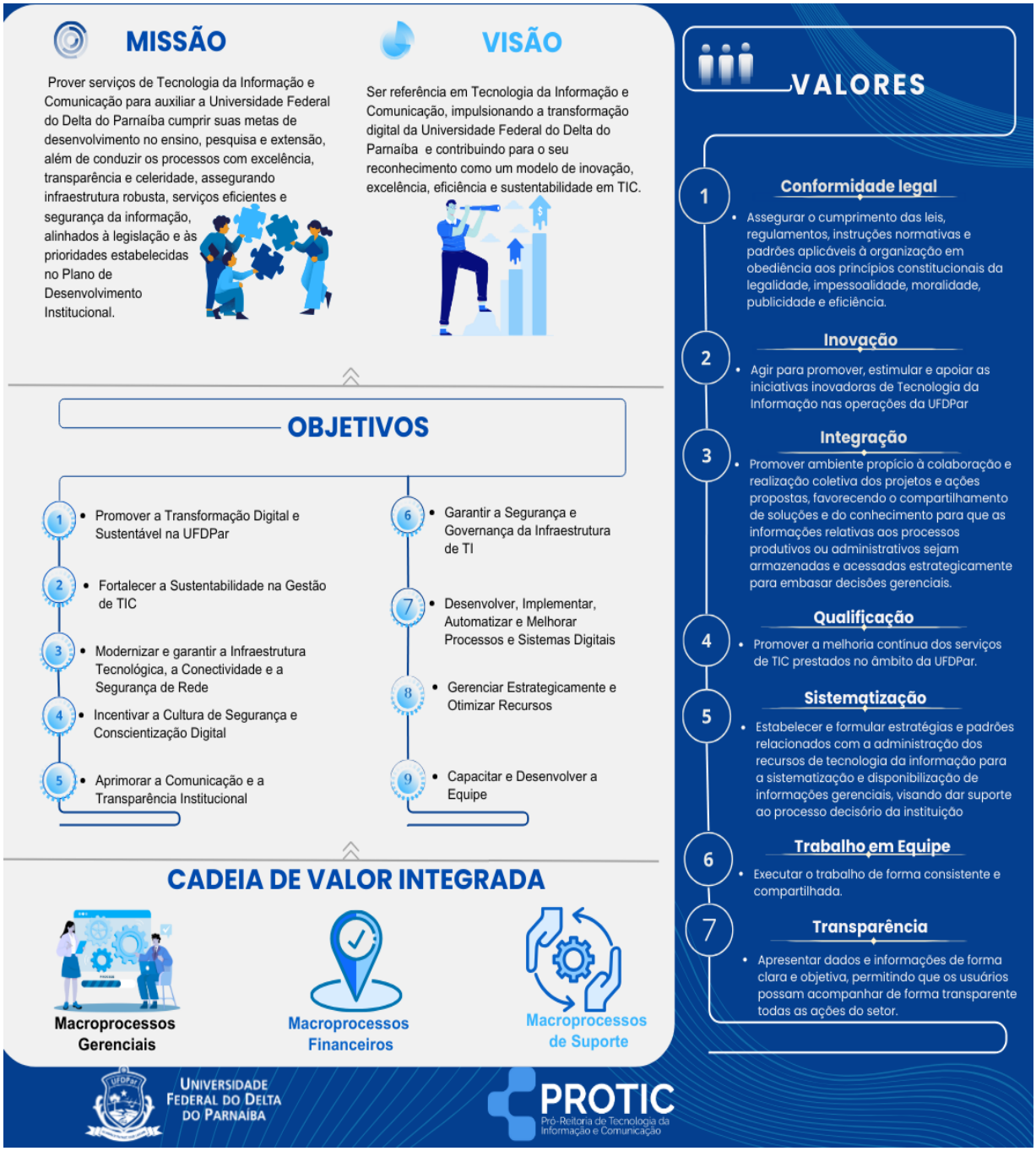
4.1.2 Mapa Estratégico

O Mapa estratégico da PROTIC, estrutura os objetivos organizacionais da unidade, a fim de orientar a atuação da PROTIC em melhorar os serviços prestados. O mapa visa alinhar os esforços da equipe da PROTIC com os Objetivos Estratégicos Institucionais, promovendo inovação, segurança da informação e governança eficiente. Desta forma, a PROTIC contribui para a modernização da gestão e na melhoria dos serviços. Todas as diretrizes estratégicas estão consolidadas na figura 15.

4.1.3 Quadro de Identificação

A apresentação do quadro de identificação (figura 15) tem como objetivo descrever sua missão, visão, valores e finalidade institucional e a estrutura hierárquica á qual está vinculada. Essa caracterização é necessária para entender o papel da PROTIC como facilitadora da transformação digital e do suporte tecnológico às atividades acadêmicas, administrativas e de pesquisa.

Figura 15: Mapa Estratégico e quadro de identificação da PROTIC



4.2 PROCESSOS DA GESTÃO DE RISCOS

4.2.1 Escala de Classificação dos Riscos

Inicialmente foi realizada a identificação dos riscos, a fim de mapear os possíveis eventos adversos que podem afetar o ambiente de TI. Para cada risco identificado, considera-se o ambiente (físico ou digital), o tipo de risco (estratégico, operacional ou orçamentário/financeiro), a causa específica e as consequências potenciais. Na avaliação, os riscos identificados foram analisados quantitativamente com base em dois critérios principais: probabilidade (P) e impacto (I). A probabilidade é classificada pelo grau de ocorrência (baixa, média ou alta), enquanto o impacto é medido pelo grau de severidade das consequências (baixo, médio ou alto). O nível de risco inerente foi calculado multiplicando esses dois fatores (P x I), resultando em uma pontuação que indica a criticidade do risco antes da aplicação de controles (Quadros 6, 7, 8, 9 e 10).

Foram também verificadas a existência de controles já implementados para mitigar os riscos identificados, com uma resposta simples: sim ou não. Caso existam controles, avalia-se sua eficácia. Quando insuficientes, são propostas medidas de melhoria. Com base na avaliação dos controles existentes, define-se a necessidade de melhorias ou a implantação de novas medidas. Essas ações são detalhadas, especificando o que será feito, como, por exemplo, a adoção de *firewalls* ou treinamentos de conscientização para os servidores. Além disso, calcula-se o Fator de Atenuação (FA), que reflete a eficácia das medidas propostas, ajustando o nível de risco residual (P x I x FA). O monitoramento contínuo dos riscos foi realizado para garantir que os controles permaneçam eficazes diante de mudanças no ambiente de TI ou do surgimento de novas ameaças. Isso envolve a revisão periódica dos riscos e a análise de indicadores, como relatórios de incidentes ou auditorias, assegurando que o nível de risco residual esteja dentro de limites aceitáveis. Em seguida, definimos a estratégia de tratamento para cada risco, escolhendo entre quatro opções: evitar (eliminar o risco), transferir (delegar a terceiros, como seguradoras), mitigar (reduzir sua probabilidade ou impacto) ou aceitar (assumir o risco quando o custo de mitigação supera os benefícios). Cada ação é atribuída a uma unidade ou subunidade responsável, com um prazo estabelecido para sua execução. A gestão de riscos da

PROTIC exige um ciclo contínuo que depende da colaboração entre as unidades responsáveis e com postura proativa para proteger os ativos da UFDPar.

Quadro 5: Análise da Probabilidade do Risco (P)

NÍVEL	GRAU DE OCORRÊNCIA	DESCRIÇÃO
1	Muito Baixa (menor que 10%)	Improvável: evento extraordinário, sem histórico de ocorrência.
2	Baixa (entre 10% e 30%)	Rara: evento casual e inesperado, sem histórico de ocorrência.
3	Média (entre 30% e 50%)	Possível: evento esperado, de frequência reduzida, com histórico de ocorrência.
4	Alta (entre 50% e 70%)	Provável: evento usual, ocorre na maioria das circunstâncias.
5	Muito Alta (entre 70% e 100%)	Praticamente certo: evento repetitivo e constante, sempre ocorre.

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

Quadro 6: Análise do Impacto do Risco (I)

NÍVEL	GRAU DE IMPACTO	DESCRIÇÃO
1	Muito Baixo	Mínimo: sem danos ou prejuízos, perda financeira pequena ou indireta.
2	Baixo	Pequeno: compromete somente o processo em questão, impacto mínimo nos objetivos.
3	Médio	Moderado: requer algum tratamento, pois indica significativa perda financeira. Há possibilidade de recuperação no caso de consequências negativas.
4	Alto	Significativo: grandes danos e prejuízos financeiros diretos, com baixa possibilidade de recuperação no caso de consequências negativas.
5	Muito Alto	Crítico: compromete fortemente os objetivos institucionais, sem possibilidade de recuperação no caso de consequências negativas.

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

Quadro 7: Avaliação dos Controles (FA)

NÍVEL	DESCRIÇÃO	FATOR
Inexistente	NÃO FORMATADO: Controle inexistente ou mal implementado	1
Fraco	FALTA SISTEMATIZAÇÃO: Controles em andamento com ações caso a caso e baseado na confiança das pessoas	0,8
Mediano	CONTROLES PARCIAIS: Para algumas causas há controle efetivo para mitigação do risco, porém para outras não há controle	0,7
Satisfatório	NECESSIDADE DE APRIMORAMENTO: há controles implementados com ações adequadas que mitigam os riscos, porém requer melhoria	0,5
Forte	SEM FALHAS DETECTADAS: ações mitigadoras de risco em todos os aspectos relevantes com controles consolidados	0,4

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

Quadro 8: Risco para (P) x (I) x (FA)

Risco Crítico (RC)	13 a 25
Risco Alto (RA)	7 a 12
Risco Moderado (RM)	4 a 6
Risco Baixo (RB)	1 a 3

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

Quadro 9: Matriz de Nível de Riscos

IMPACTO	5	**5**	**10**	**15**	**20**	**25**
	4	**4**	**8**	**12**	**16**	**20**
	3	**3**	**6**	**9**	**12**	**15**
	2	**2**	**4**	**6**	**8**	**10**
	1	**1**	**2**	**3**	**4**	**5**
		1	2	3	4	5
		PROBABILIDADE				

Fonte: Comissão elaboradora (Portaria PROTIC N° 03, de 07 de fevereiro de 2025)

4.2.2 Identificação dos Riscos

Foi realizada a identificação dos riscos, a fim de garantir a segurança, a continuidade e eficiência dos serviços de tecnologia que sustentam as atividades acadêmicas e administrativas. Neste processo, foi realizada uma análise das vulnerabilidades e ameaças que podem impactar a infraestrutura, os sistemas e os dados institucionais, considerando tanto o ambiente externo quanto o interno. A seguir, serão apresentados os riscos identificados nesses dois contextos, destacando suas características e implicações.

4.2.2.1 Ambiente externo

Quadro 10: Identificação dos riscos no ambiente externo

Tipos	IDENTIFICAÇÃO DOS RISCOS				
	Objeto Analisado	**Unidade/ Subunidade responsável**	**Risco**	**Causa(s)**	**Consequência(s)**
Macroeconômico	Baixo orçamento para investimento em TI.	PROPLAN	Comprometimento dos investimentos, aquisições e capacitações.	1. Corte orçamentário nas Universidades Federais; 2. Contingenciamento orçamentário.	1. Estagnação dos processos operacionais
Ambiental / Legal	Aquisição de bens e serviços de TIC.	PROTIC/ CDBD e PROPLAN	Dificuldade em encontrar fornecedores que atendam aos critérios de	1. Mercado restrito ou falta de exigências regulatórias claras.	1. Atrasos nas aquisições e possível comprometimento das metas de sustentabilidade.

			sustentabilidade.		
Tecnológico	Gestão de armazenamento de dados.	PROTIC/ CPPGTIC	Dependência excessiva de fornecedores externos.	1. Falta de infraestrutura interna suficiente para armazenamento.	1. Vulnerabilidade a aumentos de custo, falhas ou descontinuidade dos serviços terceirizados.
Ambiental / Legal	Gestão do descarte de resíduos tecnológicos.	PROTIC/ DSITIC e PRAD	Dificuldade em encontrar parceiros ou empresas certificadas.	1. Mercado restrito ou falta de prestadores de serviço qualificados na região.	1. Atraso no descarte adequado e possível não conformidade com normas ambientais.
Tecnológico	Capacidade de armazenamento e processamento de dados.	PROTIC	Demanda maior do que a infraestrutura consegue suportar.	1. Crescimento acelerado sem planejamento adequado.	1. Lentidão nos sistemas, falhas operacionais e necessidade urgente de ampliação.
Tecnológico	Levantamento de demandas tecnológicas.	PROTIC/ CPPGTIC/ CISI	Obsolescência rápida do levantamento devido a mudanças constantes.	1. Evolução acelerada das tecnologias e surgimento de novas necessidades.	1. Necessidade de revisões recorrentes, possíveis falhas no planejamento e alocação ineficiente de recursos.

Fonte: PROTIC (2025).

Foram identificados sete riscos externos, relacionados principalmente com fatores de dependencia de terceiros, restrições orçamentárias, sustentabilidade e dinamismo do ambiente tecnológico. Esses riscos refletem desafios exernos que exigem estratégias de mitigação para garantir a eficlência e a continuidade dos serviços de TIC.

4.2.2.2 Ambiente interno

Quadro 11: Identificação dos riscos no ambiente interno

Tipos	IDENTIFICAÇÃO DOS RISCOS				
	Objeto Analisado	**Unidade/ Subunidade responsável**	**Risco**	**Causa(s)**	**Consequência(s)**
Organizacional	Gestão e planejamento estratégico de TI.	PROTIC/ CPPGTIC	Comprometimento da continuidade e eficácia dos projetos de TI.	1. Falta de um planejamento estratégico estruturado a médio e longo prazo; 2. ausência de políticas de governança bem definidas	1. Interrupção ou atraso na implementação de projetos; 2. dificuldade na adaptação a novas demandas tecnológicas; 3. desperdício de recursos financeiros e humanos
Social	Gestão de pessoas e retenção de talentos na PROTIC.	PROTIC e PROGEP	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	1. Falta de incentivos para permanência; 2. baixa valorização profissional; 3. ausência de um plano de carreira estruturado.	1. Perda de conhecimento técnico e domínio; 2. necessidade constante de capacitação de novos servidores; 3. atrasos na execução de projetos e atividades
Organizacional	Capacidade operacional da equipe de TIC.	PROTIC/ CPPGTIC	Sobrecarga da equipe e atrasos na execução.	1. Alta demanda de projetos sem ampliação proporcional da equipe.	1. Queda na produtividade e impacto na qualidade das entregas.

Social	Mapeamento da infraestrutura de rede e conectividade.	PROTIC/ CISI	Falta de equipe comprometida para a execução eficiente.	1. Desmotivação, falta de capacitação ou acúmulo de tarefas.	1. Atrasos e possíveis falhas no mapeamento, impactando planejamentos futuros.
Legal / Financeiro	Processos administrativos para aquisição e contratação.	PROTIC/ CPPGTIC	Atrasos em licitações, autorizações e contratações de consultorias.	1. Burocracia e trâmites internos demorados.	1. Impacto no cronograma dos projetos e na execução das metas planejadas.
Social / Legal	Engajamento da comunidade acadêmica em campanhas institucionais.	PROTIC/ CCI	Baixa participação de estudantes, professores e servidores.	1. Desinteresse, comunicação ineficaz ou ausência de incentivos.	1. Impacto na efetividade das campanhas e no alcance dos objetivos propostos.
Tecnológico / Financeiro	Qualificação da equipe para implementação de novas tecnologias.	PROTIC	Falta de profissionais especializados para conduzir treinamentos e suporte.	1. Escassez de mão de obra qualificada ou ausência de capacitação interna.	1. Atrasos na adoção de novas tecnologias e necessidade de investimentos extras em capacitação ou plataformas.
Legal / Organizacional	Padronização do uso de elementos visuais institucionais.	PROTIC/ CCI	Uso indevido ou não utilização dos elementos visuais padronizados.	1. Falta de fiscalização e controle efetivo sobre a aplicação das diretrizes.	1. Inconsistência na identidade visual da instituição, impactando a comunicação e a imagem institucional.
Tecnológico	Atualização de indicadores institucionais.	PROTIC/ CS, CPPGTIC e PROPLAN	Dados desatualizados comprometem a tomada de decisão.	1. Falta de um processo de manutenção eficaz e contínuo.	1. Informações imprecisas, impactando planejamento, gestão e avaliação de desempenho.
Tecnológico / Social	Sistema de notificações institucionais.	PROTIC/ DSITIC	Excesso de notificações (spam) reduzir a efetividade do sistema	1. Falta de um controle adequado na frequência e relevância das notificações	1. Irritação dos usuários, desativação das notificações e menor engajamento com informações importantes.
Financeiro	Implementação de conformidade com boas práticas em TIC	PROTIC e PROPLAN	Custos elevados para adequação.	1. Necessidade de investimentos em infraestrutura, treinamento e consultoria.	1. Possível impacto orçamentário, atrasos na implementação e necessidade de priorização de ações.

Financeiro	Viabilidade financeira da implementação de soluções.	PROPLAN	Algumas soluções podem ser inviáveis devido a restrições orçamentárias.	1. Orçamento insuficiente para cobrir todos os investimentos necessários.	1. Atrasos na implementação, necessidade de alternativas mais baratas ou redução do escopo das iniciativas.
Tecnológico / Ambiental	Infraestrutura digital para substituição do uso de papel.	PROTIC/ CS CPPGTIC	Dificuldade na redução do uso de papel devido à falta de sistemas eficientes.	1. Infraestrutura digital inadequada ou insuficiente para suportar a transição.	1. Continuidade da dependência de documentos físicos, aumento de custos operacionais e impacto ambiental negativo.
Tecnológico	Monitoramento e coleta de dados institucionais.	PROTIC/ CS	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	1. Ausência ou infraestrutura de sistemas automatizados de monitoramento.	1. Processos manuais demorados, maior possibilidade de erros e dificuldade na análise e tomada de decisões.
Tecnológico / Legal	Segurança de softwares livres utilizados na instituição.	PROTIC e PRAD	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	1. Alguns softwares gratuitos não podem receber atualizações regulares ou suporte técnico adequado.	1. Maior exposição a ataques cibernéticos, comprometimento da integridade dos dados e necessidade de esforços extras para mitigar riscos.
Social / Organizacional	Gestão da carga de trabalho da equipe.	PROTIC	Sobrecarga da equipe, impactando a qualidade do atendimento.	1. Aumento da demanda sem o devido dimensionamento de pessoal ou otimização de processos.	1. Queda na qualidade dos serviços prestados, aumento do estresse entre os colaboradores e risco de erros operacionais.
Social / Organizacional	Capacitação dos servidores.	PROTIC e PROGEP	Dificuldade na adesão às capacitações.	1. Falta de tempo ou interesse dos servidores em participar dos treinamentos.	1. Baixo aproveitamento das capacitações, dificuldade na implementação de novas práticas e impacto na eficiência institucional.
Tecnológico	Acesso a redes, sistemas e internet	PROTIC/ CISI	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	1. Falha no provedor de internet; 2. configuração incorreta de rede; 3. ataque cibernético (ex.: DDoS);	1. Interrupção de operações críticas; 2. atrasos na comunicação; 3. perda de produtividade e impacto em serviços dependentes de conectividade.

				4. falha em equipamentos de rede (roteadores, switches).	
Tecnológico	Serviço de e-mail indisponível	PROTIC/ CISI	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	1. Falha no servidor de e-mail; 2. sobrecarga do sistema; 3. ataque de *phishing* ou *ransomware*, ou configuração inadequada.	1. Atrasos na comunicação interna e externa; 2. perda de informações importantes; 3. interrupção de processos dependentes de e-mails e possível impacto na reputação organizacional.
Tecnológico	Falha do Hardware dos servidores do DataCenter	PROTIC/ CISI	Mau funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	1. Desgaste natural de componentes; 2. superaquecimento; 3. falha no fornecimento de energia; 4. manutenção inadequada.	1. Indisponibilidade de sistemas críticos; 2. perda de dados; 3. interrupção de serviços; 4. altos custos de reparo ou substituição.
Tecnológico	Ameaças à Segurança Cibernética	PROTIC/ CISI/ DDSI	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	1. Malware, phishing, exploração de vulnerabilidades; 2. falta de atualizações de segurança; 3. comportamento inadequado de usuários.	1. Vazamento de informações sensíveis; 2. interrupção de serviços; 3. prejuízo financeiro; 4. danos à reputação da UFDPar.

Tecnológico	Interrupções por Falhas de Infraestrutura	PROTIC/ CISI e PREUNI	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	1. Falhas em sistemas de refrigeração; 2. problemas em cabeamento; 3. obsolescência de equipamentos; 4.desastres naturais.	1. Tempo de inatividade prolongado; 2. perda de dados; 3. custos elevados de recuperação; 4. impacto na continuidade dos negócios.
Ambiental	Falha no fornecimento de energia elétrica	PREUNI	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	1. Quedas de energia externas; 2. falha em geradores; 3. sobrecarga no sistema elétrico; 4. falta de manutenção.	1. Desligamento abrupto de servidores e equipamentos; 2. corrupção de dados; 3. interrupção de serviços; 4.danos físicos aos ativos.
Tecnológico/Ambiental	Superaquecimento dos ativos	PROTIC e PREUNI	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	1. Falha no sistema de refrigeração; 2. ventilação inadequada; 3. acúmulo de poeira; 4.sobrecarga operacional.	1. Redução da vida útil dos equipamentos; 2. falhas intermitentes; 3. desligamentos automáticos; 4. danos permanentes aos componentes.
Tecnológico	Falha na rotina de backup	PROTIC/ DBD	Incapacidade de realizar ou restaurar backups de dados críticos.	1. Configuração incorreta do sistema de backup; 2. falha no armazenamento; 3. falta de testes regulares; 4. erro humano.	1. Perda irreversível de dados em caso de falhas ou ataques; 2. incapacidade de restaurar operações; 3. exposição a riscos legais ou regulatórios.

Social/Tecnológico	Desinformação e Uso Indevido	PROTIC/ DDSI	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	1. Falta de treinamento dos usuários; 2. políticas de acesso mal definidas; 3. manipulação intencional.	1. Decisões baseadas em dados errôneos; 2. comprometimento da credibilidade; 3. confusão operacional; 4. possíveis sanções legais.
Tecnológico	Vazamento de Dados	PROTIC/ CISI/ DDSI	Exposição não autorizada de informações sensíveis ou confidenciais.	1. Ataques cibernéticos; 2. falhas de segurança em sistemas; 3. erro humano (ex.: envio de dados a destinatários errados); 4. falta de criptografia.	1. Perda da confiança na instituição; 2. multas regulatórias (ex.: LGPD, GDPR); 3. danos financeiros; 4. risco de litígios.
Tecnológico	Falha na prestação do serviço em nuvem	PROTIC/ DSITIC/ CISI	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	1. Falhas técnicas nos servidores do provedor; 2. falta de capacidade e escalabilidade; 3. negligência na manutenção; 4. interrupções por ataques cibernéticos ao provedor; 5. descumprimento do contrato.	1. Indisponibilidade de sistemas e dados hospedados na nuvem; 2. atrasos em processos críticos; 3. perda de produtividade; 3. custos adicionais para soluções emergenciais; 4. potencial comprometimento da continuidade dos negócios.

Social / Tecnológico	Desvio de equipamentos	PROTIC, PROPLAN e PREUNI	Furto/Roubo de equipamentos.	1. Falta de segurança física; 2. Controle de acesso insuficiente; 3. Localização em áreas de alto risco; 4. Descuido dos funcionários; 5. Ausência de sistemas de rastreamento.	1. Perda de equipamentos valiosos 2. Vazamento de dados sensíveis armazenados nos dispositivos 3. Interrupção das operações 4. Custos financeiros elevados para reposição 5. Dificuldade em recuperar os equipamentos
Tecnológico / Organizacional	Plano de ação ou resposta a incidentes.	PROTIC/ DDSI	Falha na execução do plano de ação de incidentes em situações reais.	1. Ausência de testes e simulações regulares.	1. Ineficiência na resposta a crises, maior tempo de recuperação e possíveis impactos operacionais.

Fonte: PROTIC (2025).

A análise do ambiente interno revelou um conjunto de desafios que impactam a eficiência, segurança e continuidade dos serviços tecnológicos. Esses problemas abrangem desde limitações na execução de projetos e na qualidade do atendimento, devido a sobrecarga de atividade e dificuldades em processos administrativos e carência de profissionais qualificados. A baixa adesão da comunidade acadêmica a iniciativas de capacitação, aliada A resistência à digitalização, compromete a modernização e a adoção de boas práticas. Questões como dados desatualizados, excesso de notificações e ausência de ferramentas adequadas prejudicam a gestão, enquanto restrições orçamentárias dificultam investimentos em infraestrutura. Além disso, vulnerabilidades de segurança, falhas em sistemas críticos, interrupções operacionais e riscos a integridade de dados expõem a instituição a ameaças, demandando estratégias para fortalecer a resiliência e a confiabilidade dos serviços de TIC.

4.2.3 Avaliação dos Riscos

A avaliação dos riscos relacionados à PROTIC visa identificar, analisar e gerenciar os potenciais perigos que podem comprometer a integridade, a confidencialidade e a disponibilidade dos sistemas, dados e gestão. Este processo estruturado envolve diversas etapas, como a identificação dos riscos, a avaliação de sua probabilidade e impacto, a verificação de controles existentes, a melhoria ou implantação de medidas de controle e o monitoramento contínuo dos riscos, culminando em um tratamento adequado.

4.2.3.1 Ambiente externo

Quadro 12: Avaliação dos Riscos no ambiente externo

Tipos	IDENTIFICAÇÃO DOS RISCOS	AVALIAÇÃO DOS RISCOS				
		Probabilidade (P)		Impacto (I)		Nível de Risco Inerente
	Riscos	Grau de Ocorrência	Nível	Grau de Impacto	Nível 2	P x I
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações.	Médio	3	Muito Alto	5	15
Ambiental / Legal	Dificuldade em encontrar fornecedores que atendam aos critérios de sustentabilidade.	Médio	3	Alto	4	9
Tecnológico	Dependência excessiva de fornecedores externos.	Alto	4	Alto	4	16
Ambiental / Legal	Dificuldade em encontrar parceiros ou empresas certificadas.	Médio	3	Médio	3	9
Tecnológico	Demanda maior do que a infraestrutura consegue suportar.	Alto	4	Muito Alto	5	20

Tecnológico	Obsolescência rápida do levantamento devido a mudanças constantes.	Alto	4	Médio	3	12

Fonte: PROTIC (2025).

4.2.3.2 Ambiente Interno

Quadro 13: Avaliação dos Riscos no ambiente interno

Tipos	IDENTIFICAÇÃO DOS RISCOS	AVALIAÇÃO DOS RISCOS				
		Probabilidade (P)		Impacto (I)		Nível de Risco Inerente
	Riscos	Grau de Ocorrência	Nível	Grau de Impacto	Nível 2	P x I
Organizacional	Comprometimento da continuidade e eficácia dos projetos de TI.	Médio	3	Alto	4	12
Social	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	Baixo	2	Baixo	2	4
Organizacional	Sobrecarga da equipe e atrasos na execução.	Alto	4	Alto	4	16
Social	Falta de equipe comprometida para a execução eficiente.	Médio	3	Médio	3	9
Legal / Financeiro	Atrasos em licitações, autorizações e contratações de consultorias.	Alto	4	Alto	4	16
Social / Legal	Baixa participação de estudantes, professores e servidores.	Médio	3	Médio	3	9
Tecnológico / Financeiro	Falta de profissionais especializados para conduzir treinamentos e suporte.	Alto	4	Alto	4	16
Legal / Organizacional	Uso indevido ou não utilização dos elementos visuais padronizados.	Médio	3	Baixo	2	6

Tecnológico	Dados desatualizados comprometem a tomada de decisão.	Médio	3	Médio	3	9
Tecnológico / Social	Excesso de notificações (spam) reduzir a efetividade do sistema	Médio	3	Médio	3	9
Financeiro	Custos elevados para adequação.	Médio	3	Alto	4	12
Financeiro	Algumas soluções podem ser inviáveis devido a restrições orçamentárias.	Alto	4	Alto	4	16
Tecnológico / Ambiental	Dificuldade na redução do uso de papel devido à falta de sistemas eficientes.	Médio	3	Médio	3	9
Tecnológico	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	Médio	3	Alto	4	12
Tecnológico / Legal	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	Médio	3	Alto	4	12
Social / Organizacional	Sobrecarga da equipe, impactando a qualidade do atendimento.	Alto	4	Alto	4	16
Social / Organizacional	Dificuldade na adesão às capacitações.	Médio	3	Médio	3	9
Tecnológico	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	Baixo	2	Muito Alto	5	10
Tecnológico	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	Baixo	2	Alto	4	8
Tecnológico	Mau funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	Baixo	2	Muito Alto	5	10
Tecnológico	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	Alto	4	Muito Alto	5	20
Tecnológico	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	Baixo	2	Muito Alto	5	10

Ambiental	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	Médio	3	Muito Alto	5	15
Tecnológico/Ambiental	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	Médio	3	Alto	4	12
Tecnológico	Incapacidade de realizar ou restaurar backups de dados críticos.	Baixo	2	Muito Alto	5	10
Social/Tecnológico	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	Médio	3	Médio	3	9
Tecnológico	Exposição não autorizada de informações sensíveis ou confidenciais.	Baixo	2	Muito Alto	5	10
Tecnológico	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	Médio	3	Alto	4	12
Social / Tecnológico	Furto/Roubo de equipamentos.	Muito Baixo	1	Muito Alto	5	5
Tecnológico / Organizacional	Falha na execução do plano de ação de incidentes em situações reais.	Médio	3	Alto	4	12

Fonte: PROTIC (2025)

4.2.4 Verificação dos Controles Existentes

Nesta fase, identificamos e avaliamos os controles com o objetivo de reunir e analisar as principais ações, políticas, planos, ferrramentas e procedimentos que propiciem o controle dos riscos de forma a direcionar aas atividades da PROTIC e asssim contribuir para obtenção dos resultados e cumprimento dos objetivos e diretrizes estratégicas da PROTIC, alinhado às institucionais. A análise concentrasse em verificar a existência de normas e mecanismos formais que orientam a execuçao dos processo, especialmente aqueles que estão sujeitos à interfereencia de eventos que possam comprometer seu desempenho e integridade.

4.2.4.1 Ambiente Externo

Quadro 14 - Verificação de controle de riscos no ambiente externo

Tipos	IDENTIFICAÇÃO DOS RISCOS Riscos	VERIFICAÇÃO DE CONTROLES DE RISCOS Existência de Controle (POSSIBILIDADES DE RESPOSTAS: SIM OU NÃO)
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações.	NÃO
Ambiental / Legal	Dificuldade em encontrar fornecedores que atendam aos critérios de sustentabilidade.	NÃO
Tecnológico	Dependência excessiva de fornecedores externos.	NÃO
Ambiental / Legal	Dificuldade em encontrar parceiros ou empresas certificadas.	NÃO
Tecnológico	Demanda maior do que a infraestrutura consegue suportar.	NÃO
Tecnológico	Obsolescência rápida do levantamento devido a mudanças constantes.	NÃO

Fonte: PROTIC (2025).

4.2.4.2 Ambiente interno

Quadro 15 - Verificação de controle de riscos no ambiente interno

Tipos	IDENTIFICAÇÃO DOS RISCOS Riscos	VERIFICAÇÃO DE CONTROLES DE RISCOS Existência de Controle (POSSIBILIDADES DE RESPOSTAS: SIM OU NÃO)
Organizacional	Comprometimento da continuidade e eficácia dos projetos de TI.	NÃO
Social	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	NÃO
Organizacional	Sobrecarga da equipe e atrasos na execução.	NÃO
Social	Falta de equipe comprometida para a execução eficiente.	NÃO
Legal / Financeiro	Atrasos em licitações, autorizações e contratações de consultorias.	NÃO

Social / Legal	Baixa participação de estudantes, professores e servidores.	NÃO
Tecnológico / Financeiro	Falta de profissionais especializados para conduzir treinamentos e suporte.	NÃO
Legal / Organizacional	Uso indevido ou não utilização dos elementos visuais padronizados.	NÃO
Tecnológico	Dados desatualizados comprometem a tomada de decisão.	NÃO
Tecnológico / Social	Excesso de notificações (spam) reduzir a efetividade do sistema	NÃO
Financeiro	Custos elevados para adequação.	NÃO
Financeiro	Algumas soluções podem ser inviáveis devido a restrições orçamentárias.	NÃO
Tecnológico / Ambiental	Dificuldade na redução do uso de papel devido à falta de sistemas eficientes.	NÃO
Tecnológico	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	NÃO
Tecnológico / Legal	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	NÃO
Social / Organizacional	Sobrecarga da equipe, impactando a qualidade do atendimento.	NÃO
Social / Organizacional	Dificuldade na adesão às capacitações.	SIM
Tecnológico	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	SIM
Tecnológico	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	NÃO
Tecnológico	Mau funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	SIM
Tecnológico	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	SIM
Tecnológico	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	NÃO
Ambiental	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	SIM
Tecnológico/Ambiental	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	NÃO
Tecnológico	Incapacidade de realizar ou restaurar backups de dados críticos.	SIM
Social/Tecnológico	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	NÃO
Tecnológico	Exposição não autorizada de informações sensíveis ou confidenciais.	NÃO

Tecnológico	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	NÃO
Social / Tecnológico	Furto/Roubo de equipamentos.	SIM
Tecnológico / Organizacional	Falha na execução do plano de ação de incidentes em situações reais.	NÃO

Fonte: PROTIC (2025).

Com base na análise dos riscos edentificados, há fragilidades que podem comprometer a efetividade e a sustentabilidade das operações da UFDPar. Os riscos envolvem desde limitações estruturais e tecnológicas até desafios de cadeia de suprimentos. Além disso, a obsolência acererada das informações evidencia a necessidade de mecanismos mais dinâmicos de atualização e revisão. Estes e os demais riscos identificados, se não forem adequadamente gerenciados, podem afetar negativamente a UFDPar, a capacidade de resposta e a continuidade dos serviços de TIC.

4.2.5 Melhoramento e Eventual Implementação de Controles

Com o objetivo de fortalecer a gestão de riscos, foi elaborada a tabela de Melhoramento e Eventual Implementaçao de Controles para os ambientes externo e interno. Nesta, apresentamos um conjunto abrangente de medidas corretivas e preventivas aplicáveis aos riscos identificados. Essas ações foram pensadas para mitigar vulnerabilidades, promover maior resilieencia operacional e garantir a continuidade dos seviços essenciais, considerando aspectos como infraetrutura, fornecedores, processos, pessoas e segurança da inforação. A tabela contempla dsde mecanismos de planejamento estratégico até controles técnicos e organizacionais, detalhando intervenções específicas para cada tipo de risco mapeado. Essa abordagem sistematizada permite alinhar os controles com as boas práticas de governança, sustentabilidade e inovação tecnológica.

4.2.4.1. Ambiente Externo

Quadro 16 - Melhoria e/ou implantação de medidas de controle de riscos no ambiente externo

	Risco	MELHORIA E/OU IMPLANTAÇÃO DE MEDIDAS DE CONTROLE DE RISCOS			
		Medidas de Melhoria de Controles Existentes	Medidas de Controle a serem implementadas	Avaliação de Controles Existentes	
				Fator	(P x I x FA)
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações.	NÃO	1. Planejamento interno de investimento frente a demanda do setor	1	15
Ambiental / Legal	Dificuldade em encontrar fornecedores que atendam aos critérios de sustentabilidade.	NÃO	1. Certificação prévia de fornecedores; 2. cláusulas de sustentabilidade nos contratos; 3. banco de dados de fornecedores sustentáveis.	1	9
Tecnológico	Dependência excessiva de fornecedores externos.	NÃO	1. Cadastro de fornecedores alternativos; 2. simulações de interrupção de fornecimento; 3. contratos com penalidades por falhas.	1	16
Ambiental / Legal	Dificuldade em encontrar parceiros ou empresas certificadas.	NÃO	1. Mapeamento prévio de empresas certificadas, parcerias com associações setoriais, avaliação trimestral de editais.	1	9

Tecnológico	Demanda maior do que a infraestrutura consegue suportar.	NÃO	1. Monitoramento em tempo real da infraestrutura; 2. expansão modular de capacidade; 3. priorização de demandas críticas.	1	20
Tecnológico	Obsolescência rápida do levantamento devido a mudanças constantes.	NÃO	1. Sistema de gestão de mudanças; 2. revisões ágeis trimestrais; 3. alerta de obsolescência.	1	12

Fonte: PROTIC (2025).

4.2.4.2 Ambiente Interno

Quadro 17 - Melhoria e/ou implementação de medidas de controle de riscos no ambiente interno

	Risco	**MELHORIA E/OU IMPLANTAÇÃO DE MEDIDAS DE CONTROLE DE RISCOS**			
		Medidas de Melhoria de Controles Existentes	**Medidas de Controle a serem implementadas**	**Avaliação de Controles Existentes**	
				Fator	**(P x I x FA)**
Organizacional	Comprometimento da continuidade e eficácia dos projetos de TI.	NÃO	1. Monitoramento semanal dos marcos do projeto; 2. checklist de conformidade com prazos.	1	12

Social	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	NÃO	1. Revisão mensal dos indicadores de desempenho; 2. implementação de acordos de nível de serviço; 3. treinamento contínuo da equipe.	1	4
Organizacional	Sobrecarga da equipe e atrasos na execução.	NÃO	1. Redimensionamento da equipe conforme a demanda; 2. automação de processos; 3. capacitação contínua	1	16
Social	Falta de equipe comprometida para a execução eficiente.	NÃO	1. Programa de reconhecimento; 2. feedback contínuo; 3. metas claras e mensuráveis.	1	9
Legal / Financeiro	Atrasos em licitações, autorizações e contratações de consultorias.	NÃO	1. Automação de etapas do processo licitatório; 2. reuniões semanais de acompanhamento; 3. checklist de documentos.	1	16
Social / Legal	Baixa participação de estudantes, professores e servidores.	NÃO	1. Enquetes de interesse; 2. eventos de divulgação; 3. incentivos à participação	1	9
Tecnológico / Financeiro	Falta de profissionais especializados para conduzir treinamentos e suporte.	NÃO	1. Banco de especialistas terceirizados; 2. programa de formação interna;	1	16

			3. avaliação de competências.		
Legal / Organizacional	Uso indevido ou não utilização dos elementos visuais padronizados.	NÃO	1. Auditoria trimestral de uso da identidade visual; 2. Modelos obrigatórios; 3. penalidades por uso indevido.	1	6
Tecnológico	Dados desatualizados comprometem a tomada de decisão.	NÃO	1. Rotina automática de atualização de dados; 2. validação cruzada mensal; 3. alerta de dados obsoletos.	1	9
Tecnológico / Social	Excesso de notificações (spam) reduzir a efetividade do sistema	NÃO	1. Filtros personalizados por usuário; 2. limite de notificações diárias; 3. análise de relevância.	1	9
Financeiro	Custos elevados para adequação.	NÃO	1. Planejamento financeiro detalhado; 2. busca por subsídios; 3. priorização de investimentos.	1	12
Financeiro	Algumas soluções podem ser inviáveis devido a restrições orçamentárias.	NÃO	1. Matriz de priorização de projetos, 2. parcerias para redução de custos; 3. uso de soluções open-source.	1	16
Tecnológico / Ambiental	Dificuldade na redução do uso de papel	NÃO	1. Digitalização de processos;	1	9

	devido à falta de sistemas eficientes.		2. treinamento em ferramentas digitais.		
Tecnológico	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	NÃO	1. Implantação de software de coleta de dados; 2. integração de sistemas existentes; 3. validação periódica dos dados.	1	12
Tecnológico / Legal	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	NÃO	1. Atualizações automáticas de software; 2. política de fim de vida útil.	1	12
Social / Organizacional	Sobrecarga da equipe, impactando a qualidade do atendimento.	NÃO	1. Sistema de triagem de demandas; 2. limite de atendimentos por funcionário; 3. suporte de chatbots.	1	16
Social / Organizacional	Dificuldade na adesão às capacitações.	SIM, de certificação obrigatória	1. Cursos online assíncronos; 2. gamificação do aprendizado; 3. certificação obrigatória.	0,7	9
Tecnológico	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	SIM, implantando Zabbix	1. Configurar alerta em tempo real para quedas de ping ou latência alta em links de internet e redes internas; 2. Testar periodicamente a redundância de conexões; 3. Registrar logs de desempenho de roteadores e switches.	0,5	10

Tecnológico	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	NÃO	1. Verificar continuamente a disponibilidade do serviço com testes automatizados; 2. Configurar alerta para falhas de autenticação ou atrasos na entrega de mensagens; 3. Analisar logs de erros no servidor de e-mail.	1	8
Tecnológico	Mau funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	SIM, software de monitoramento de servidor.	1. Configurar alerta para paradas inesperadas ou sobrecarga; 2. Testar regularmente sistemas de *failover*.	0,5	10
Tecnológico	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	SIM, *firewall* avançado.	1. Analisar logs de tráfego de rede para identificar padrões suspeitos; 2. Realizar varreduras regulares de vulnerabilidades; 3. Implementar autenticação multifator e monitoramento de acesso não autorizado.	0,8	20
Tecnológico	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	NÃO	1. Monitorar condições físicas do ambiente (ex.: ar-condicionado, cabeamento); 2. Realizar inspeções preventivas regulares na infraestrutura; 3. Configurar alerta para falhas em equipamentos críticos.	1	10
Ambiental	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	SIM, nobreaks e gerador	1. Verificar a situação de carga e autonomia do UPS em tempo real; 2. Testar a ativação automática de geradores periodicamente;	0,5	15

			3. Configurar alerta para quedas de energia ou falhas no sistema de backup.		
Tecnológico/Ambiental	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	NÃO	1. Monitorar a temperatura ambiente e dos equipamentos em tempo real; 2. Configurar alerta para níveis críticos de calor; 3. Realizar manutenção preventiva em sistemas de refrigeração.	1	12
Tecnológico	Incapacidade de realizar ou restaurar backups de dados críticos.	SIM, relatório diário de situação.	1. Verificar o sucesso de *backups* diários automatizados via logs; 2. Testar restaurações periodicamente em ambiente controlado; 3. Configurar alerta para falhas ou atrasos nos processos de *backup*.	0,5	10
Social/Tecnológico	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	NÃO	1. Monitorar logs de uso de sistemas por usuários; 2. Realizar treinamentos regulares e auditorias de comportamento; 3. Configurar alerta para atividades anômalas;	1	9
Tecnológico	Exposição não autorizada de informações sensíveis ou confidenciais.	NÃO	1. Monitorar tentativas de acesso ou extração de dados sensíveis; 2. Auditar permissões de acesso a informações críticas; 3. Configurar alerta para movimentação não autorizada de arquivos.	1	10

Tecnológico	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	NÃO	1. Integrar monitoramento em tempo real com APIs dos provedores de nuvem; 2. Configurar alerta para quedas de desempenho ou interrupções reportadas; 3. Testar planos de contingência.	1	12
Social / Tecnológico	Furto/Roubo de equipamentos.	Sim, Sistema de monitoramento por câmeras, Segurança Patrimonial e Grades	1. Instalar alarmes e fechaduras eletrônicas; 2. Treinamento regular sobre segurança e políticas de supervisão de equipamentos.	0,5	5
Tecnológico / Organizacional	Falha na execução do plano de ação de incidentes em situações reais.	NÃO	1. Treinamentos práticos regulares; 2. testes de stress do plano em condições simuladas; 3. checklist de validação pré-execução; 4. Checklist de recursos pré-incidente; 5. Protocolos flexíveis para imprevistos; 6. Registro e análise pós-incidente.	1	12

Fonte: PROTIC (2025).

As medidas de controle propostas representam uma maturidade da gestão de riscos da PROTIC. Ao contemplar soluções de curto, médio e longo prazo – com foco no planejamento, monitoramento contínuo, capacitaçao e automação – a PROTIC se posiciona de forma mais preparada para prevenir falhas, responder a imprevistos e garantir a conformidade com o PDI da UFDPar. A implementassão destes controles contribui para o uso mais eficiente dos recursos pela comunidade acadêmica e a melhoria da qualidade dos serviços. A adoção sistemática dessas ações deve ser acompanhada por ciclos regulares de revisão e aprimoramento, a fim de assegurar sua efetividade frente ás constantes mudanças dos ambientes.

4.2.6 Monitoramento dos Riscos

No processo de monitoramento de riscos, realiza-se o acompanhamento contínuo dos eventos identificados, com o objetivo de revisar e atualizar suas classificações sempre que mudanças internas ou externas alterarem o cenário de exposição. Essa etapa permite a realocação dos níveis de probabilidade e impacto, inicialmente atribuídos aos riscos, variações no ambiente ou entrada de novos dados. O monitoramento é essencial para assegurar que a valiação dos riscos permaneça alinhada á realidade operacional da PROTIC, permitindo ajustes ágeis e embasados nas decisões estratégicas.

4.2.6.1. Ambiente Externo

Quadro 18: Monitoramento dos riscos no ambiente externo

Tipos	**IDENTIFICAÇÃO DOS RISCOS**	**MONITORAMENTO DOS RISCOS**
	Riscos	**Relação de medidas (relatórios, documentos, portifólios, entre outros)**
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações.	1. Relatórios de Atividades Anuais

Ambiental / Legal	Dificuldade em encontrar fornecedores que atendam aos critérios de sustentabilidade.	1. Portfólio de fornecedores avaliados; 2. política de compras sustentáveis.
Tecnológico	Dependência excessiva de fornecedores externos.	1. Plano de contingência, diversificação de fornecedores.
Ambiental / Legal	Dificuldade em encontrar parceiros ou empresas certificadas.	1. Relatório de parceiros certificados.
Tecnológico	Demanda maior do que a infraestrutura consegue suportar.	1. Relatório de capacidade da infraestrutura e escalabilidade.
Tecnológico	Obsolescência rápida do levantamento devido a mudanças constantes.	1. Relatórios de atualização.

4.2.6.2 Ambiente Interno

Quadro 19: Monitoramento dos riscos no ambiente interno

Tipos	**IDENTIFICAÇÃO DOS RISCOS** **Riscos**	**MONITORAMENTO DOS RISCOS** **Relação de medidas (relatórios, documentos, portifólios, entre outros)**
Organizacional	Comprometimento da continuidade e eficácia dos projetos de TI.	1. Elaboração de um Plano de Continuidade de Negócios; 2. Relatórios de acompanhamento de projetos; 3. auditorias internas.
Social	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	1. Indicadores de desempenho; 2. plano de qualidade; 3. relatórios de incidentes.
Organizacional	Sobrecarga da equipe e atrasos na execução.	1. Plano de capacidade da equipe; 2. relatórios de horas trabalhadas.
Social	Falta de equipe comprometida para a execução eficiente.	1. Plano de engajamento e avaliação de desempenho.
Legal / Financeiro	Atrasos em licitações, autorizações e contratações de consultorias.	1. Relatórios de situação de processos.
Social / Legal	Baixa participação de estudantes, professores e servidores.	1. Relatórios de engajamento.
Tecnológico / Financeiro	Falta de profissionais especializados para conduzir treinamentos e suporte.	1. Relatório de capacitação interna.
Legal / Organizacional	Uso indevido ou não utilização dos elementos visuais padronizados.	1. Manual de identidade visual, treinamentos.
Tecnológico	Dados desatualizados comprometem a tomada de decisão.	1. Relatórios de atualização e validação de dados.
Tecnológico /		1. Relatórios de uso do sistema.

Social	Excesso de notificações (spam) reduzir a efetividade do sistema	
Financeiro	Custos elevados para adequação.	1. Relatório de revisão de orçamento e análise de custo benefício.
Financeiro	Algumas soluções podem ser inviáveis devido a restrições orçamentárias.	1. Relatório de priorização e análise de alternativas de baixo custo.
Tecnológico / Ambiental	Dificuldade na redução do uso de papel devido à falta de sistemas eficientes.	1. Relatórios de uso de papel.
Tecnológico	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	1. Relatório de necessidades.
Tecnológico / Legal	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	1. Relatórios de segurança.
Social / Organizacional	Sobrecarga da equipe, impactando a qualidade do atendimento.	1. Relatório de redistribuição de tarefas.
Social / Organizacional	Dificuldade na adesão às capacitações.	1. Relatórios de adesão.
Tecnológico	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	1. Relatório de disponibilidade de rede (uptime, latência, pacotes perdidos); 2. Relatório de incidentes de conectividade (data, duração, causa).
Tecnológico	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	1. Relatório de Desempenho do Sistema de E-mails (taxa de entrega, falhas); 2. Relatório de incidentes de E-mail (tempo de parada, impacto).
Tecnológico	mAu funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	1. Relatório de saúde dos servidores (CPU, memória, disco); 2. Relatório de paradas não planejadas (causa, tempo de recuperação).
Tecnológico	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	1. Relatório de análise de vulnerabilidades (resultados de varreduras); 2. Relatório de incidentes de segurança (ataques detectados, resposta); 3. Política de segurança da informação; 4. Plano de resposta a incidentes Cibernéticos; 5. Matriz de riscos de segurança (ameaças vs. controles).
Tecnológico	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	1. Relatório de condições da infraestrutura física; 2. Relatório de manutenção preventiva; 3. Plano de manutenção da infraestrutura física; 4. Inventário de ativos físicos críticos;

		5. Layout dos equipamentos no datacenter; 6. Checklist de inspeção física mensal.
Ambiental	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	1. Relatório de situação do UPS e geradores; 2. Relatório de testes de energia reserva; 3. Plano de Contingência Energética; 4. Contrato de manutenção de equipamentos de energia; 5. Esquema elétrico do sistema de energia de backup; 6. Registro de interrupções e ativações do gerador.
Tecnológico/Ambiental	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	1. Relatório de monitoramento térmico (temperaturas registradas); 2. Relatório de falhas de refrigeração (incidentes e ações); 3. Política de controle de Temperatura no datacenter; 4. Cronograma de manutenção de sistemas de climatização; 5. Mapa térmico do ambiente de TI; 6. Logs de sensores de temperatura.
Tecnológico	Incapacidade de realizar ou restaurar backups de dados críticos.	1. Relatório de situação de *backups* (sucesso, falhas, tempo); 2. Relatório de testes de restauração; 3. Política de *backup* e restauração; 4. Plano de recuperação de dados; 5. Catálogo de dados críticos; 6. Evidências de *backups* bem-sucedidos.
Social/Tecnológico	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	1. Relatório de uso de sistemas (atividades suspeitas ou anômalas); 2. Relatório de treinamento de usuários; 3. Registro de permissões de acesso por usuário; 4. Auditoria de logs de acesso e alterações.
Tecnológico		1. Relatório de auditoria de acesso a dados sensíveis;

	Exposição não autorizada de informações sensíveis ou confidenciais.	2. Relatório de Incidentes de vazamento; 3. Política de proteção de dados; 4. Matriz de classificação de informações; 5. Inventário de dados sensíveis.
Tecnológico	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	1. Relatório de desempenho de serviços em nuvem; 2. Relatório de incidentes reportados pelo provedor; 3. Contrato com o provedor de nuvem; 4. Plano de contingência para falhas na nuvem; 5. Mapa de dependências de serviços em nuvem; 6. Histórico de situação do provedor
Social / Tecnológico	Furto/Roubo de equipamentos.	1. Relatório de instalação de equipamentos de segurança, de monitoramento, de treinamento, de conformidade, de recuperação, e ativos rastreados; 2. Portfólio de Incidentes, de Treinamento; 3. Política de Controle de Acesso 4. Plano de Contingência
Tecnológico / Organizacional	Falha na execução do plano de ação de incidentes em situações reais.	1. Plano de resposta a emergências; 2. Relatórios pós-incidente; 3. Portfólio de Cenários de Incidentes; 4. Manual de Treinamento;

Fonte: PROTIC (2025).

O monitoramento proposto será conduzido com base nas estratégias de controle e mitigação previamente apresentadas, as quais abrangem ações planejadas para minimizar os riscos identificados. Essas medidas, estruturadas de forma integrada e preventiva, orientarão o acompanhamento contínuo dos riscos, permitindo ajustes nos níveis de probabilidade e impacto sempre que necessario, garantindo maior efetividade.

4.2.7 Revisão dos Riscos

A revisão dos riscos será conduzida de forma sistematica e adaptável, com foco na reavaliação dos níveis de probabilidade e dos impactos inerentes aos riscos previamente identificados, sempre que houver alterações nos contextos interno e externo da PROTIC. Essa reavaliação permitirá ajustar o tratamento dos riscos á medida que novos dados forem disponibilizados, controles forem implementados ou ambiente apresentar mudanças. A atualização das classificações visa manter a gestão de riscos sempre alinhada á realidade operacional, garantindo respostas mais ágeis, coerentes e eficazes diante de possíveis ameaças.

A periodicidade dessas revisões será definida conforme o grau de complexidade e a variabilidade do comportamento dos riscos observados. Para riscos mais dinãnicos ou de alto impacto, as análises serão realizadas com maior frequeencia – podendo ser trimestral ou mensal -, enquanto riscos mais estáveis poderão ser revisados semestral ou anualmente. Além disso, revisões extraordinárias poderão ser realizadas sempre que eventos relevantes ocorrerem, com mudanças tecnológicas, reformulações ou incidentes críticos. Essa abordagem flexiível garante que a PROTIC esteja continuamente preparada para mitigar riscos e promover a melhoria contínua dos seus processos.

4.2.8 Tratamento dos Riscos

As tabelas de tratamento de riscos apresentadas a seguir, reúnem de forma estruturada as ações propostas para enfrentar, reduzir ou eleimiar os risocs identificados. Essa etapa é fundamental para a consolidação de uma gestão da PROTIC proativa, permitindo definir respostas adequadas a cada risco com base em sua criticidade e impacto potencial. As medidas de tratamento foram elaboradas considerando critérios técnicos, viabilidade operacional e alinhamento com os objetivos estratégicos, contemplando alternativas como mitigação, aceitação, transfereencia o eliminação dos riscos. Com isso, busca-se promover maior segurança, eficiência e sustentabilidade nas operações, fortaleceno a capacidade de resposta diante de cenarios adversos.

4.2.8.1. Ambiente Externo

Quadro 20 - Tratamento do risco externo

Tipo	IDENTIFICAÇÃO DOS RISCOS	TRATAMENTO DO RISCO					
		Tipo de Risco			Ações de Tratamento		
	Riscos	Estratégico	Operacional	Orçamentário / Financeiro	Ação	Unidade/ Subunidade responsável	Prazo
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações.	SIM	SIM	SIM	ACEITAR	PROPLAN	12 Meses
Ambiental / Legal	Dificuldade em encontrar fornecedores que atendam aos critérios de sustentabilidade.	SIM	NÃO	NÃO	TRANSFERIR	PROTIC/ CDBD e PROPLAN	6 meses
Tecnológico	Dependência excessiva de fornecedores externos.	SIM	NÃO	NÃO	MITIGAR	PROTIC/ CPPGTIC	12 Meses
Ambiental / Legal	Dificuldade em encontrar parceiros ou empresas certificadas.	SIM	NÃO	NÃO	MITIGAR	PROTIC/ DSITIC e PRAD	6 meses
Tecnológico	Demanda maior do que a infraestrutura consegue suportar.	NÃO	SIM	NÃO	MITIGAR	PROTIC	3 meses
Tecnológico	Obsolescência rápida do levantamento devido a mudanças constantes.	SIM	NÃO	NÃO	MITIGAR	PROTIC/ CPPGTIC/ CISI	3 meses

Fonte: PROTIC (2025).

4.2.8.2. Ambiente Interno

Quadro 21 - Tratamento do risco interno

Tipos	IDENTIFICAÇÃO DOS RISCOS	TRATAMENTO DO RISCO					
		Tipo de Risco			Ações de Tratamento		
	Riscos	Estratégico	Operacional	Orçamentário / Financeiro	Ação	Unidade/ Subunidade responsável	Prazo
Organizacional	Comprometimento da continuidade e eficácia dos projetos de TI.	SIM	SIM	NÃO	MITIGAR	PROTIC / CPPGTIC	3 meses
Social	Impacto na continuidade dos projetos e na qualidade dos serviços de TI.	NÃO	SIM	NÃO	MITIGAR	PROTIC e PROGEP	3 meses
Organizacional	Sobrecarga da equipe e atrasos na execução.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CPPGTIC	1 Mês
Social	Falta de equipe comprometida para a execução eficiente.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CISI	3 meses
Legal / Financeiro	Atrasos em licitações, autorizações e contratações de consultorias.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CPPGTIC	1 Mês
Social / Legal	Baixa participação de estudantes, professores e servidores.	SIM	NÃO	NÃO	MITIGAR	PROTIC/ CCI	6 meses
Tecnológico / Financeiro	Falta de profissionais especializados para conduzir treinamentos e suporte.	NÃO	SIM	NÃO	TRANSFERIR	PROTIC	12 Meses
Legal / Organizacional	Uso indevido ou não utilização dos elementos visuais padronizados.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CCI	3 meses
Tecnológico	Dados desatualizados comprometem a tomada de decisão.	SIM	NÃO	NÃO	MITIGAR	PROTIC/ CS/ CPPGTIC e PROPLAN	1 Mês
Tecnológico / Social	Excesso de notificações (spam) reduzir a efetividade do sistema	NÃO	SIM	NÃO	MITIGAR	PROTIC/ DSITIC	1 Mês
Financeiro	Custos elevados para adequação.	NÃO	NÃO	SIM	ACEITAR	PROTIC e PROPLAN	12 Meses
Financeiro	Algumas soluções podem ser inviáveis devido a restrições	NÃO	NÃO	SIM	MITIGAR	PROPLAN	6 meses

	orçamentárias.						
Tecnológico / Ambiental	Dificuldade na redução do uso de papel devido à falta de sistemas eficientes.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CS/ CPPGTIC	12 Meses
Tecnológico	Dificuldade na coleta de dados devido à falta de ferramentas adequadas.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CS	6 meses
Tecnológico / Legal	Possíveis vulnerabilidades devido à falta de suporte e atualizações.	NÃO	SIM	NÃO	MITIGAR	PROTIC e PRAD	1 Mês
Social / Organizacional	Sobrecarga da equipe, impactando a qualidade do atendimento.	NÃO	SIM	NÃO	MITIGAR	PROTIC	3 meses
Social / Organizacional	Dificuldade na adesão às capacitações.	NÃO	SIM	NÃO	MITIGAR	PROTIC e PROGEP	6 meses
Tecnológico	Perda de conectividade com redes internas ou externas, impossibilitando o acesso a sistemas e serviços online.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CISI	3 Meses
Tecnológico	Falha no funcionamento do sistema de e-mails, impedindo envio e recebimento de mensagens.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CISI	2 Meses
Tecnológico	Mau funcionamento ou parada total dos servidores que sustentam os serviços do DataCenter.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CISI	4 Meses
Tecnológico	Exposição a ataques maliciosos que comprometem a integridade, confidencialidade ou disponibilidade de dados e sistemas.	SIM	SIM	NÃO	MITIGAR	PROTIC/ CISI/ DDSI	6 Meses
Tecnológico	Paralisação de operações devido a problemas na infraestrutura física ou tecnológica.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ CISI e PREUNI	4 Meses
Ambiental	Interrupção no abastecimento de energia que mantém os sistemas operacionais.	NÃO	SIM	NÃO	MITIGAR	PREUNI	4 Meses
Tecnológico/Ambiental	Aumento excessivo da temperatura de equipamentos, como servidores e dispositivos de TI.	NÃO	SIM	NÃO	MITIGAR	PROTIC e PREUNI	3 Meses
Tecnológico	Incapacidade de realizar ou restaurar backups de dados críticos.	NÃO	SIM	NÃO	EVITAR	PROTIC/ DBD	3 Meses
Social/Tecnológico	Disseminação de informações incorretas ou uso inadequado de sistemas e dados.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ DDSI	2 Meses

Tecnológico	Exposição não autorizada de informações sensíveis ou confidenciais.	SIM	NÃO	NÃO	EVITAR	PROTIC/ CISI/ DDSI	3 Meses
Tecnológico	Degradação ou interrupção nos serviços de computação em nuvem fornecidos por uma empresa terceirizada.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ DSITIC/ CISI	3 Meses
Social / Tecnológico	Furto/Roubo de equipamentos.	SIM	SIM	SIM	MITIGAR E TRANSFERIR	PROTIC, PROPLAN e PREUNI	3 Meses
Tecnológico / Organizacional	Falha na execução do plano de ação de incidentes em situações reais.	NÃO	SIM	NÃO	MITIGAR	PROTIC/ DDSI	3 Meses

Fonte: PROTIC (2025).

As medidas propostas visam não apenas mitigar os riscos identificados, mas também fortalecer os processos internos, garantir a continuidade das operações e promover maior confiabilidade nos serviços prestados. Ao integrar ações estruturadas de controle, monitoramento e capacitação, a PROTIC se posiciona de forma estratégica para enfrentar os desafios, responder a imprevistos e alcançar seus objetivos com maior segurança e resiliência. A efetividade desse tratamento dependerá da implementação consistente das ações, da revisão periódica dos cenários de risco e da integração contínua entre planejamento, execução e avalição.

5. RESULTADOS

A realização de um diagnóstico detalhado revela-se um passo para a avaliação crítica da continuidade ou interrupção dos planos e execuções em curso, além de proporcionar uma oportunidade para refletir sobre os progressos alcançados e aprofundar a compreensão do contexto organizacional. Esse processo permite não apenas identificar o alinhamento das ações implementadas com os objetivos estratégicos, mas também reconhecer eventuais desvios que demandem ajustes ou reformulações.

5.1 Resultados obtidos no PGR 2023-2025

Este resultado representa a avaliação e execução do PGR da PROTIC no período de 2023 a 2025, com base na análise das ações realizadas. O objetivo é verificar o grau de cumprimento das medias previstas no plano anterior, com foco na efetividade as ações adotadas para o tratamento dos riscos identificados. A partir desta análise, foram reformuladas algumas estratégias para o PGR 2025-2027 e o aprimoramento contínuo da gestão de riscos, aproximando continuamente o planejamento das rotinas administrativas da unidade e fortalecendo a aderência aos objetivos estratégicos da UFDPar.

A metodologia aplicada nesta avaliação consistiu na revisão detalhada do PGR 2023 – 2025, com a finalidade de compreender os riscos previamente identificados aos quais a PROTIC estava exposta. A partir dessa revisão, foram extraídas informações com os objetivos estratégicos associados, o planejamento das ações, os níveis de impacto e a probabilidade, bem como as medidas de controle e tratamento propostas. Em seguida, foi realizada a verificação prática das ações que foram efetivamente executadas, com o intuito de avaliar sua coerência com o planejamento inicial e sua capacidade de mitigar ou eliminar os riscos.

Os resultados evidenciam avanços no tratamento dos riscos, com a realização de 81,82% das ações previstas alcançadas, resultando na eliminação ou redução dos riscos a níveis considerados aceitáveis. Chegamos a 13,64% das ações redirecionadas com o descarte de inservíveis de TIC, a avaliação dos servidores e equipamentos desatualizados, fatores que necessitam de maior alinhamento da PROTIC com a Unidade de Recursos Humanos, além da restrição orçamentária

governamental, a qual atenuou a probabilidade de investimentos para atualização dos equipamentos. Tivemos 1 ação não alcançada, relacionada com os impactos ambientais nocivos produzidos pela TIC, que corresponde a 4,54%. Este, além de associado a necessidade de investimentos, também necessita de ações para mitigar o consumo de energia e organização de descarte de inservíveis.

De modo geral, o PGR 2023 – 2025 contribuiu para o fortalecimento da gestão de riscos da PROTIC, sobretudo na racionalização do uso de recursos orçamentários e na valorização da capacitação contínua da equipe técnica, especialmente diante da incorporação de novos servidores para a tecnologia da informação e governança da unidade. Destaco que o ambiente organizacional positivo, favorece a colaboração entre os profissionais da unidade. Contudo, persistem desafios a serem superados, como o gerenciamento adequado de resíduos oriundos da rápida obsolescência de equipamento de TIC e a necessidade e criação de canais mais eficientes de escuta e comunicação com os usuários. Enfrentar essas questões será fundamental par aa elaboração de execução deste novo ciclo do PGR, com maior maturidade e alinhamento a demandas institucionais.

Quadro 22: Demonstração dos resultados

Tipos	**IDENTIFICAÇÃO DOS RISCOS**	**Resultados**
	Riscos	
Macroeconômico	Comprometimento dos investimentos, aquisições e capacitações da PROTIC	ALCANÇADO
Ambiental	Acúmulo para descarte dos resíduos de TIC	REDIRECIONADO
Social	Dificuldade para avaliação dos servidos prestados pela PROTIC na instituição	REDIRECIONADO
Social	Menor rendimento e qualidade dos serviços da PROTIC	ALCANÇADO
Social	GAP dos demais setores do papel e as funções de TIC dentro da instituição.	ALCANÇADO
Tecnológico	Dependência, Lentidão e baixa soluções que envolve os sistemas externo e interno e não operacionalização dentro da instituição	ALCANÇADO
Tecnológico	Desatualização dos equipamentos de TI da instituição;	REDIRECIONADO
Tecnológico	Ineficiência operacional.	ALCANÇADO
Legal	A não operacionalidade dos sistemas em conformidade com as exigências legais	ALCANÇADO
Financeiro	Estagnação das operações dentro da TI	ALCANÇADO
Ambiental	Impactos ambientais nocivos;	NÃO ALCANÇADO

Ambiental	Potenciais problemas legais e de saúde pública.	ALCANÇADO
Social	Dificuldade na adaptação e integração dos membros;	ALCANÇADO
Social	Falta de colaboração e sinergia entre os membros.	ALCANÇADO
Social	Falta do diagnóstico dos pontos críticos para execução das atividades internas buscando a eficiência, eficácia e efetividade.	ALCANÇADO
Social	1. Atrasos ou falhas no atendimento das demandas de responsabilidades do setor.	ALCANÇADO
Social	1. Ineficiência operacional e a falta de especialização adequada para as tarefas.	ALCANÇADO
Social	1. Dificuldade na adoção de melhorias ou inovações necessárias para o crescimento e aprimoramento do setor.	ALCANÇADO
Tecnológico	1. Inoperação dos sistemas necessários para a instituição, prejudicando a tomada de decisões estratégicas.	ALCANÇADO
Legal	1. Falta de documentos orientativos institucionais do setor	ALCANÇADO
Legal	1. Sobrecarga de trabalho e ineficiência do setor.	ALCANÇADO
Legal	1. Despreparação da equipe frente às demandas do setor.	ALCANÇADO

Fonte: PROTIC (2025).

6. CONSIDERAÇÕES FINAIS

O Plano de Gestão de Riscos implementado no âmbito PROTIC destaca-se pela priorização de macroprocessos críticos que sustentam a operacionalidade institucional. Dentre esses macroprocessos, sobressaem-se os sistemas acadêmicos, as redes de comunicação e os serviços digitais, elementos que constituem a base estrutural para o desempenho eficiente e contínuo das atividades da UFDPar. A estruturação desse plano permitiu, ainda, a consolidação de um conjunto robusto de informações e documentação detalhada acerca dos mecanismos de controle interno, os quais proporcionam uma análise sistemática e organizada das vulnerabilidades presentes no ambiente tecnológico da instituição. Tal abordagem favorece a transparência nos processos, ao mesmo tempo, em que viabiliza a alocação otimizada de esforços e recursos, direcionando-os de forma precisa e assertiva para os riscos que exigem intervenção imediata, com base em uma avaliação hierarquizada de prioridades.

O Plano de Gestão de Riscos fortalece a governança no âmbito da PROTIC, posicionando-a como um agente de promoção da modernização e da sustentabilidade da UFDPar. Esse fortalecimento é evidenciado pelo aprimoramento da infraestrutura

tecnológica, que passa a operar em consonância com melhores padrões de qualidade, e em alinhamento estratégico, com os objetivos institucionais de longo prazo. Como resultado, cria-se um ambiente organizacional mais resiliente, dotado de maior capacidade de resposta frente a desafios emergentes, como ameaças cibernéticas e a ampliação da dependência de soluções digitais no contexto acadêmico e administrativo.

Para consolidar e ampliar os resultados já alcançados, a PROTIC visualiza ações futuras para fortalecer a gestão de riscos. Dentre elas, o investimento em ferramentas de monitoramento em tempo real para identificar e responder rapidamente as ameaças cibernéticas e falhas operacionais. Soluções com base em inteligência artificial podem ser integradas para prever riscos potenciais com base em padrões de comportamento, reduzindo o tempo de resposta e minimizando os impactos. Além disso, ampliaremos nossos programas de treinamento e atualização para as equipes de TI e demais membros da comunidade acadêmica envolvidos nos macroprocessos críticos. Esses programas abordam temas como novas ameaças cibernéticas, conformidade com regulamentações de proteção de dados e melhores práticas em segurança da informação, garantindo que o capital humano esteja preparado para lidar com os desafios emergentes. Outro ponto é a realização de exercícios periódicos de simulação de cenários de crise, como ataques cibernéticos, falhas de infraestrutura ou interrupções nos serviços digitais. Esses testes permitem avaliar a eficácia dos planos de contingência e identificar pontos de melhoria nos processos de resposta de recuperação.

7. REFERÊNCIAS

BRASIL. Tribunal de Contas da União. Manual de gestão de riscos do TCU / Tribunal de Contas da União. – Brasília: TCU, Secretaria de Planejamento, Governança e Gestão (Seplan), 2020.

BRASIL. Universidade Federal do Delta do Parnaíba. Conselho Universitário. Resolução nº 002, de 14 de outubro de 2020. Aprova o Plano de Integridade da Universidade Federal do Delta do Parnaíba (UFDPar). Disponível em: https://www.ufpi.br/arquivos_download/arquivos/Parnaiba/2021/ufdpar-plano-deintegridade.pdf. Acesso em 28 de fevereiro de 2025.

BRASIL. Universidade Federal do Delta do Parnaíba. Pró-Reitoria de Planejamento. MANUAL DE ORIENTAÇÕES DE PROCESSOS DE GESTÃO DE RISCOS DA UFDPar. UFDPar, Parnaíba. 2022.

BRASIL. Universidade Federal do Delta do Parnaíba. Pró-Reitoria de Planejamento. POP PROPLAN 01 013 A Elaboração do Plano de Gestão de Riscos. Disponível em: https://ufdpar.edu.br/proplan/paginas/arquivos/pop-proplan-01_013_a_elaboracao-do-plano-de-gestao-de-riscos.pdf Acesso em 10 de março de 2025.

ABNT NBR ISO 31000, Gestão de riscos — Diretrizes, 1 – 17, 2018.

ABNT NBR ISO/IEC 27701, Técnicas de segurança, Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação — Requisitos e diretrizes, 1 – 82, 2019.

ABNT NBR ISO/IEC 27005, Segurança da informação, segurança cibernética e proteção à privacidade — Orientações para gestão de riscos de segurança da informação,1 – 75, 2023

Martinsons, M. G., Davison, R. M., e Tse, D. K. (1999). The Balanced Scorecard: A Foundation for the Strategic Management of Information Systems. *Decision Support Systems*, 25(1), 71-88. Disponível em: https://www.sciencedirect.com/science/article/abs/pii/S0167923698000864?via%3Dihub. Acesso em 2 de março de 2025.