



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PIAUÍ
SUPERINTENDÊNCIA DE TECNOLOGIA DA
INFORMAÇÃO- STI**



DOCUMENTO DE QUALIFICAÇÃO DA DEMANDA

Setor Requisitante (Unidade/Setor/Departamento): SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO	
Responsável pela Demanda: Mário Cristiano Lopes de Moura	Matrícula SIAPE: 1773588
E-mail: sti@ufpi.edu.br	Telefone: (86) 3215-5627
Objeto da futura contratação: AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO (BACKUP)	
O objeto da contratação está previsto no Plano de Contratações Anual [2025], conforme detalhamento a seguir:	
ID PCA no PNCP:	ID do item no PCA:
Data de publicação no PNCP:	Classe/Grupo:
Identificador da futura contratação:	Código do PDM do Item:
Caso o objeto da contratação NÃO conste no Plano de Contratações Anual, apresentar justificativa pela não inserção da demanda conforme prazo estabelecido no art. 6º do Decreto nº 10.947/2022.	
Em conformidade com o Decreto nº 10.947, de 25 de janeiro de 2022, a UFPI elaborou e submeteu seu Plano Anual de Contratações para o ano de 2025, observando o prazo estabelecido no art. 6º do referido decreto. O referido planejamento foi consolidado com base nas necessidades e prioridades identificadas à época, visando a otimização dos recursos e o alinhamento com os objetivos estratégicos da instituição. Contudo, o cenário de segurança da informação, tanto em âmbito nacional quanto global, sofreu uma abrupta e acelerada deterioração em um período posterior à fase de consolidação do PAC, tornando a demanda por uma solução robusta de backup uma necessidade crítica e inadiável. A não inclusão da presente demanda no PAC se fundamenta na materialização de um novo contexto de risco, cuja dimensão e iminência não poderiam ser razoavelmente previstas durante o ciclo de planejamento ordinário. A justificativa assenta-se em dois pilares principais: A) Do Cenário de Ameaças Cibernéticas: Frequência e Severidade Elevadas Durante o último ano, observou-se uma escalada sem precedentes na frequência e sofisticação de ataques cibernéticos, especialmente do tipo <i>ransomware</i>, direcionados a instituições do setor público e de educação. Relatórios de agências de segurança nacionais e internacionais indicam que estes ataques evoluíram de simples sequestros de dados para operações de exfiltração e dupla extorsão, visando paralisar completamente as operações da entidade-alvo e expor dados sensíveis. As IFES, que custodiam um vasto volume de dados críticos – incluindo dados pessoais de milhares de alunos e servidores (em conformidade com a LGPD), pesquisas científicas de valor inestimável, informações financeiras e acervos acadêmicos históricos –, tornaram-se alvos prioritários. A interrupção dos sistemas acadêmicos e administrativos, ou a perda permanente desses dados, representaria um prejuízo irreparável para a continuidade das atividades essenciais desta UFPI e para o patrimônio público. A natureza imprevisível e a rápida evolução dessas ameaças configuram um fato superveniente, que alterou fundamentalmente o cálculo de risco da instituição. A mitigação deste risco, que anteriormente poderia ser tratada com soluções paliativas, agora exige uma resposta tecnológica de nível corporativo, com funcionalidades como imutabilidade de backups, versionamento avançado e recuperação rápida em caso de desastre (Disaster Recovery), características não previstas como urgentes no planejamento original. B) Das Exigências Atuais do Ministério da Gestão e da Inovação (MGI) e da Política de Segurança da Informação (PPSI) O Governo Federal, por meio do Ministério da Gestão e da Inovação em Serviços Públicos (MGI) e da Secretaria de Governo Digital, tem intensificado as diretrizes e normativos relacionados à segurança da informação e à governança de dados no âmbito do SISP (Sistema de Administração dos Recursos de Tecnologia da Informação). As exigências atuais extrapolam a mera existência de uma Política de Segurança da Informação (PPSI) formal. As novas orientações e auditorias do sistema de controle enfatizam a necessidade de comprovação da eficácia dos controles de segurança, sendo a capacidade de restauração de serviços e dados (continuidade de negócios) um dos itens de maior relevância. Uma política de backup eficaz, que garanta a integridade, confidencialidade e disponibilidade dos dados, é um pilar fundamental para a resiliência cibernética exigida.	



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PIAUÍ
SUPERINTENDÊNCIA DE TECNOLOGIA DA
INFORMAÇÃO- STI**



A contratação de uma solução de backup moderna não é mais apenas uma boa prática de TI, mas um requisito mandatório para o cumprimento das normativas federais e para a adequação da Universidade à Estratégia Nacional de Segurança Cibernética. Adiar esta contratação para o próximo ciclo do PAC implicaria em manter a instituição em estado de não conformidade e vulnerabilidade inaceitável por um período prolongado.

Diante do exposto, conclui-se que a necessidade de contratação de uma solução de backup corporativo robusta é uma demanda nova, de caráter urgente e imprevisível, surgida após o encerramento do prazo de planejamento do PAC 2025. A sua não realização imediata submete esta IFES a um nível de risco operacional e estratégico inaceitável.

1. Descrição da demanda.

AQUISIÇÃO DE SOLUÇÃO DE PROTEÇÃO (BACKUP)

2. Justificativa da necessidade da aquisição/ contratação de serviços, considerando o Planejamento Estratégico, se for o caso.

A presente justificativa fundamenta-se na criticidade dos ativos de informação para o cumprimento da missão institucional da Universidade Federal do Piauí e na necessidade de conformidade com as melhores práticas de governança de TI e com as exigências dos órgãos de controle, notadamente o TCU e a CGU.

A UFPI, no fiel cumprimento de sua missão basilar, apoiada no tripé ensino, pesquisa e extensão, depende intrinsecamente de seus sistemas de informação para operar. Os dados digitais constituem o ativo mais valioso e estratégico da instituição, englobando: A) Dados Acadêmicos: Registros de alunos, matrículas, históricos escolares, notas, dados de egressos e sistemas de gestão de ensino (SIGAA). B) Dados Administrativos: Sistemas de gestão de pessoas (folha de pagamento, dados funcionais), finanças (orçamento, contratos), patrimônio e almoxarifado (SIPAC). C) Dados de Pesquisa: Bases de dados de projetos de pesquisa, propriedade intelectual, publicações científicas e dados coletados em laboratórios. D) Dados de Extensão e Comunicação: Registros de projetos, portais institucionais, sistemas de eventos e repositórios digitais.

A indisponibilidade, perda ou corrupção de qualquer um desses conjuntos de dados resultaria em paralisação das atividades finalísticas e administrativas da Universidade, com graves prejuízos financeiros, operacionais, legais e de imagem.

Deste modo, a ausência de uma solução de backup robusta, centralizada e auditável expõe a Universidade a uma gama de riscos, dos quais podemos enumerar as falhas de hardware e software, erro humano, ataques cibernéticos cada vez mais frequentes e desastres naturais ou sinistros.

A contratação de uma solução de backup é a principal medida de controle para mitigar tais riscos, sendo um componente essencial do Plano de Continuidade de Negócios (PCN) e do Plano de Recuperação de Desastres (PRD) de qualquer organização.

Além disso, a jurisprudência do Tribunal de Contas da União (TCU) e as orientações da Controladoria-Geral da União (CGU) são claras quanto à responsabilidade dos gestores públicos em assegurar a governança e a segurança dos ativos de tecnologia da informação.

3. Em caso de contrato vigente, indicar a data de encerramento da vigência contratual.

Não há contrato vigente.

4. Previsão de data em que deve ser iniciada a contratação.

04/09/2025

5. Indicação do(s) membro(s) da equipe de planejamento e o(s) responsável(is) pela fiscalização do contrato/ata de registro de preços (*Todos os membros da equipe de planejamento e da gestão do contrato/ata de registro de preço devem assinar as declarações de ciência*)

Equipe de Planejamento da Contratação	Equipe da Gestão Contratual/Ata de Registro de Preços
1. Mário Cristiano Lopes de Moura mclmoura@ufpi.edu.br Coordenação de Infraestrutura Coordenador de Infraestrutura	1. Mário Cristiano Lopes de Moura mclmoura@ufpi.edu.br Coordenação de Infraestrutura Coordenador de Infraestrutura
2. Arinaldo Lopes da Silva arinaldo@ufpi.edu.br Coordenação de Infraestrutura	2. Arinaldo Lopes da Silva arinaldo@ufpi.edu.br Coordenação de Infraestrutura



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PIAUÍ
SUPERINTENDÊNCIA DE TECNOLOGIA DA
INFORMAÇÃO- STI**



Chefe da Divisão de Segurança da Informação/STI	Chefe da Divisão de Segurança da Informação/STI
3. Joara da Silva Araujo joara@ufpi.edu.br Superintendência de Tecnologia da Informação Assistente em Administração	4. Joara da Silva Araujo joara@ufpi.edu.br Superintendência de Tecnologia da Informação Assistente em Administração
DECLARO que estou ciente de que os servidores indicados reúnem as competências necessárias à completa execução das etapas de planejamento da contratação e fiscalização contratual, conforme disposto no art. 22, § 1º e art. 41, IN SEGES/MPDG nº 05/2017.	
Teresina, 02 de setembro de 2025. CLÉDJAN TORRES DA COSTA Assinatura Autoridade Máxima do Setor Requisitante	



**MINISTÉRIO DA EDUCAÇÃO
UNIVERSIDADE FEDERAL DO PIAUÍ
SUPERINTENDÊNCIA DE TECNOLOGIA DA
INFORMAÇÃO- STI**



**DECLARAÇÃO DOS INTEGRANTES DA EQUIPE DE PLANEJAMENTO DA
CONTRATAÇÃO**

Declaro ciência da minha indicação para integrar a equipe de Planejamento da Contratação em referência, assim como das minhas respectivas atribuições enquanto integrante com conhecimentos técnicos do setor requisitante.

Mário Cristiano Lopes de Moura

Arinaldo Lopes da Silva

Joara Araújo da Silva

DECLARAÇÃO DOS INTEGRANTES DA EQUIPE DE FISCALIZAÇÃO

Declaro que estou ciente da minha indicação para compor a equipe de Gestão/Fiscalização referente à aquisição/contratação especificada, bem como das atribuições a mim conferidas, conforme orientações contidas no Manual de Fiscalização de Contratos da PRAD, disponível no link: <https://ufpi.br/fiscalizacao-contrato-gc><https://ufpi.br/fiscalizacao-contrato-gc>.

Mário Cristiano Lopes de Moura

Arinaldo Lopes da Silva

Joara Araújo da Silva