

FUNDACAO UNIVERSIDADE FEDERAL DO PIAUI

Documento de Formalização da Demanda 297/2025

Número do Documento de Formalização da Demanda: 297/2025

1. Informações Gerais

Área requisitante	Data da conclusão da contratação	UASG	Editado por
Superintendência de Tecnologia da Informação	04/09/2025 00:00	154048	ANA MARIA DA SILVA
Descrição sucinta do objeto			
Aquisição de solução de backup para a Universidade Federal do Piauí			

2. Justificativa de Necessidade

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. Materiais/Serviços

3.1 Materiais

Nº do item	Classe	PDM	Descrição	Qtd	Val. unit. (R\$)	Val. total (R\$)
1	Computadores	Servidor	armazenamento sas: com discos sas, armazenamento sata: com discos sata, armazenamento ssd: com discos ssd, fonte alimentação: redundante (swap/hot plug), garantia on site: superior 48, interface rede lan: no mínimo 8, interface rede san: sem san, memória ram: 32, núcleos por processador: 8, processadores físicos: 1, sistema operacional: sem sistema operacional, tipo: rack	1,001	110.589,32	1.110.589,32
Unidade de fornecimento: Unidade						

3.2 Serviços

Nº do item	Grupo	Descrição	Qtd	Val. unit. (R\$)	Val. total (R\$)
1	Serviços De Manutenção E Reparo De Produtos Fabricados De Metal, Maquinaria E Equipamentos	Serviços de Instalação de Equipamentos de TI (Computadores e seus Periféricos)	2,00	25.800,00	51.600,00
2	Serviços De Manutenção E Reparo De Produtos Fabricados De Metal, Maquinaria E Equipamentos	Serviços de Instalação de Equipamentos de TI (Computadores e seus Periféricos)	1,00	32.850,00	32.850,00
3	Serviços De Manutenção E Reparo De Produtos Fabricados De Metal, Maquinaria E Equipamentos	Serviços de Instalação de Equipamentos de TI (Computadores e seus Periféricos)	80,00	650,00	52.000,00
4	Serviços De Licenciamento E Contratos De Transferência De Tecnologia	Cessão Temporária de Direitos Sobre Programas de Computador Locação de Software	20,00	54.000,00	1.080.000,00

4. Responsáveis

Todas as assinaturas eletrônicas seguem o horário oficial de Brasília e fundamentam-se no §3º do Art. 4º do [Decreto nº 10.543, de 13 de novembro de 2020](#).

Despacho: Representante da Superintendência de Tecnologia da Informação.

MARIO CRISTIANO LOPES DE MOURA
Membro da comissão de contratação

5. Acompanhamento

Id	Acompanhamento	Responsável	Data
1	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 ransomware, 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. 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.	ANA MARIA DA SILVA	02/09 /2025 14:04

6. Relacionamentos

Nenhum relacionamento encontrado.