



TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Praça Desembargador Edgard Nogueira, S/Nº - Centro Cívico - Bairro Cabral - CEP 64000920 - Teresina - PI

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA / 2022 - SEINF

1. Identificação da Área Demandante da Solução

| Unidade | CODIN | Data | 26/01/2022 |
|---------------------------------|-------------------------------------|----------------------|--------------|
| Nome do Projeto | Aquisição de solução de Datacenter | | |
| Responsável pela Demanda | Antônio Manoel Silveira de Sousa | | |
| E-mail do Responsável | codin@tre-pi.jus.br | Telefone | 86 2107-9762 |
| Integrante Demandante | Antônio Manoel Silveira de Sousa | | |
| E-mail do Integrante Demandante | codin@tre-pi.jus.br | Telefone | 86 2107-9762 |
| Fonte de Recursos | 0100 – RECURSOS DO TESOURO NACIONAL | Custo Estimado (R\$) | |

2. Objeto da Contratação

Aquisição de solução de Datacenter certificado padrão TIER III ou superior para abrigar a infraestrutura de tecnologia da informação do TRE-PI, garantindo níveis mínimos de segurança e disponibilidade.

3. Objetivo Estratégico (PETRE ou PDTI)

OE1 - Aumentar a satisfação dos usuários dos serviços de TI

OE2 - Promover a transformação digital

OE7 - Aprimorar a segurança da informação e proteção de dados

OE8 - Entregar serviços de infraestrutura e soluções corporativas

4. Motivação/Justificativa

A **segurança da informação** é um bem diretamente relacionado aos negócios da organização. Seu principal objetivo é garantir o funcionamento da organização diante de possibilidades de incidentes, evitando prejuízos, aumentando a produtividade e a disponibilidade, provendo maior qualidade aos usuários e evidenciando a reputação da organização.

O Datacenter é um ambiente centralizado, onde funcionam os equipamentos servidores de rede, de aplicação e de sistemas, ativos de comunicação e equipamentos responsáveis pelo armazenamento dos dados e informações, que atendem a demanda da organização, possuindo a finalidade adstrita a proteger e manter funcionais os equipamentos de informática críticos que compõem o núcleo do seu parque tecnológico e os dados nele inseridos.

Assim, a construção desses ambientes de **missão crítica** seguros significa proteger informações para garantir a **continuidade dos negócios** e potencializar sua eficiência.

Uma vez que neles estão instalados todos os principais equipamentos de informática e dados, o regular funcionamento de seus sistemas de segurança e sua manutenção são imprescindíveis para a continuidade dos serviços providos pela organização.

Se, por uma falha, uma interrupção não programada (*downtime*) é gerada e o Datacenter "sai do ar", as informações corporativas se tornam indisponíveis, causando custos relacionados à:

- perda ou corrupção de dados;
- queda na produtividade;
- danos a equipamentos;
- custo de reparação do problema e identificação de suas causas;
- repercussões legais;
- e impactos negativos à imagem da instituição.

Por esses motivos, é cada vez mais comum encontrarmos quem invista em soluções de ambientes com **elevada confiabilidade**. Para que um Datacenter realmente proteja as informações e mantenha sua disponibilidade, deve atender normas específicas que determinam os critérios de segurança. Uma das normas mais representativas na atualidade é a **ANSI/EIA/TIA-942**. A TIA (Telecommunications Industry Association) é uma organização americana que representa a indústria global de tecnologia da informação e da comunicação, desenvolvendo normas e pesquisas para o setor.

Em resumo, a TIA-942 especifica os requisitos para a infraestrutura de Datacenters de acordo com o grau que oferecem de **disponibilidade** e **redundância** – a repetição de equipamentos essenciais para que uns substituam os outros em caso de falhas, evitando interrupções no funcionamento.

Para isso, a norma estabelece quatro níveis de redundância e disponibilidade de Data Centers: TIER I, TIER II, TIER III e TIER IV, tendo por finalidade avaliar a performance do Datacenter, verificando se ele oferece disponibilidade de processamento conforme as necessidades da organização.

Por atuar em **negócio crítico** (organização e execução de eleições), este Tribunal necessita garantir a disponibilidade e segurança de seus ativos, sistemas e dados. Assim, faz-se necessária a utilização de ambientes seguros e com alta disponibilidade, o que seria atendido pelos padrões **TIER III** e **TIER IV**.

O Conselho Nacional de Justiça (CNJ), através do Guia da Estratégia nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD -), apresenta como boa prática advinda da antiga ENTIC-JUD (Res. CNJ nº 211/2015) que cada Órgão viabilize "1 (um) ambiente de processamento central (Data Center) com requisitos mínimos de segurança e de disponibilidade estabelecidos em normas nacionais e internacionais, que abrigue os equipamentos principais de processamento e de armazenamento de dados; de segurança e ativos de rede centrais, para maximizar a segurança e a disponibilidade dos serviços essenciais e de sistemas estratégicos do órgão".

A recomendação do CNJ e a necessidade do Tribunal tornam premente a adoção de ações no sentido de viabilizar a aquisição de solução adequada de Datacenter e que permita ao Tribunal oferecer aos seus usuários um serviço de qualidade pelos próximos anos.

5. Metas do Planejamento Estratégico a serem alcançadas

KR1.3 - Aumentar o índice de satisfação dos usuários com os serviços de TI para 95% até 2026

KR2.1 - Atingir 100% de execução do Plano de Transformação Digital até 2026

KR7.1 - Implementar a gestão de riscos em 100% dos serviços críticos até 2022

KR7.2 - Atender a 100% dos requisitos da LGPD até 2026

Teresina, 28 de janeiro de 2022.



Documento assinado eletronicamente por **Antonio Manoel Silveira de Sousa, Coordenador**, em 28/01/2022, às 11:35, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Carlos Alberto Ribeiro do Nascimento Junior, Chefe de Seção**, em 28/01/2022, às 11:45, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **Lucy Gabrielli Oliveira Simeao Aquino, Analista Judiciário**, em 16/02/2022, às 09:17, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1429892** e o código CRC **1775733E**.