DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA / 2023 - NSCIB

1. Identificação da Área Demandante da Solução

Unidade	CODIN	**Data**	21/10/2022
Nome do Projeto	Contratação de licença de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory) e servidores de arquivos em nuvem ou on-premisses.		
Responsável pela Demanda	ROSEMBERG MAIA GOMES		
E-mail do Responsável	rosemberg.maia@tre-pi.jus.br	**Telefone**	(86) 2107-9762
Integrante Demandante	ROSEMBERG MAIA GOMES		
E-mail do Integrante Demandante	rosemberg.maia@tre-pi.jus.br	**Telefone**	(86) 2107-9762
Fonte de Recursos	**0100 – RECURSOS DO TESOURO NACIONAL**	**Custo Estimado (R$)**	**2.797.456,00**

2. Objeto da Contratação

Contratação de empresa especializada para o fornecimento de licenciamento de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory) e servidores de arquivos em nuvem ou on-premisses; contemplando o monitoramento de usuários em tempo real, identificando desvios de comportamento além e permitir delegação de gerenciamento de acesso aos proprietários dos dados, executando ações proativas em múltiplos objetos, identificando e classificando conteúdos sensíveis. Incluindo licenciamento, instalação, treinamento, garantia e suporte técnico para a solução.

3. Objetivo Estratégico (PETRE ou PDTI)

Fortalecer a segurança do processo eleitoral

Aprimorar os mecanismos de transparência, segurança e acesso à informação

4. Motivação/Justificativa

O aumento exponencial de ataques cibernéticos da atualidade faz com que os órgãos da Justiça Eleitoral busquem novas soluções de proteção dos dados, uma vez que esta justiça especializada coleta, produz, trata, processa e armazena uma grande quantidade de dados diariamente, tanto on-premise como em nuvem, que necessitam ser monitorados, classificados e protegidos.

Por esse motivo, as diretrizes da Estratégia Nacional de Cibersegurança da JE (2021 a 2024), definidas pelo Tribunal Superior Eleitoral (TSE), possui como uma das iniciativas promover investimentos para contratação de soluções de segurança da informação, com a finalidade mitigar o risco de ataques cibernéticos.

Portanto, consideramos necessário e urgente o uso de ferramentas e soluções que ofereçam recursos de monitoramento contínuo, detecção, investigação e tratamento de incidentes relacionados ao acesso às informações institucionais; além de eficiência para prover um ambiente computacional aderente aos controles de segurança da informação.

Segundo o instituto de pesquisas técnicas e análises de tendências de TI – o GARTNER GROUP, cerca de 80% dos dados estratégicos das instituições estão armazenados em base de dados não estruturadas ou semiestruturadas. Além disso, o GARTNER GROUP já apresentou um estudo apontando que, em média, para cada 1 TeraByte de arquivos, existem 50.000 (cinquenta mil) pastas. Todas estas pastas armazenam dados que são usados no dia-a-dia pelos usuários e que as respectivas pastas contém arquivos com informações de conteúdo crítico ao funcionamento da instituição ou ainda dados protegidos pela Lei Geral de Proteção de dados – LGPD. Neste contexto, faz-se necessária aquisição de Solução que permita o Controle e Auditoria para servidores de dados não estruturados on-premisse e em nuvem.

Conforme levantamento realizado pela STI, diversas informações do Tribunal estão distribuídas em pastas (departamentais, setoriais ou individuais) localizadas no Data Center do Tribunal ou na nuvem do Google Workspace, que são acessadas pelos diversos usuários da rede e gerenciadas por sistemas operacionais que geram registros de eventos (logs). O tratamento, correlação, análise e investigação desses registros é algo custoso e pouquíssimo informativo, não proporcionando a devida granularidade para pesquisas de auditoria referente a quem, quando, onde e como um dado é utilizado.

Dessa forma, torna-se necessário o monitoramento de acesso e alteração dos dados armazenados, o gerenciamento e auditoria do repositório de usuários e e-mails, visando a tomada de ações proativas em casos de incidentes de segurança cibernética, ataques de malwares, ransomwares, ou até mesmo a identificação de acessos indevidos de usuários internos mal intencionados. Sem os referidos recursos de auditoria, as equipes de resposta a incidentes cibernéticos ficam reféns da utilização de uma interface gráfica bastante ineficiente ou limitada que muitas vezes não é capaz de entregar as informações necessárias à análise forense. Sem informações precisas sobre os incidentes não é possível dar as respostas eficientes aos cenários de risco cibernético e, consequentemente, não é possível endereçar os tratamentos adequados.

Outro importante fator que deve ser mencionado é o volume de informações que a auditoria nativa das ferramentas de gestão de serviço de diretório, autenticação e gerenciamento de usuários armazena (AD - Microsoft). Com o volume de dados custodiados na infraestrutura

mantida pelo Tribunal, se torna complexa a administração dos dados, demandando longos períodos de tempo, dificultando a atividade de auditoria do ambiente. Sem a solução de auditoria o cenário beira à impossibilidade de monitoramento, ao passo que contando com a solução a ser contratada as ações de monitoramento e detecção de incidentes serão simplificadas, tornando-se ágeis e precisas as demandas relacionadas à segurança do órgão.

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

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

Teresina, 18 de dezembro de 2023.

Documento assinado eletronicamente por **Rosemberg Maia Gomes**, **Coordenador de Desenvolvimento e Infraestrutura**, em 18/12/2023, às 14:37, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **Leonardo Saraiva e Silva**, **Analista Judiciário**, em 18/12/2023, às 14:39, 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 **0001978064** e o código CRC **5ADA3253**.