TRIBUNAL REGIONAL ELEITORAL DO DF

DOCUMENTO DE OFICIALIZAÇÃO DA DEMANDA – DOD
(DEMANDA PREVISTA NO PAA)

AQUISIÇÃO DE BENS E/OU SERVIÇOS (INCLUSIVE STIC)

1. IDENTIFICAÇÃO DA DEMANDA PREVISTA NO PLANO ANUAL DE AQUISIÇÕES

OBJETO TRATA-SE DE: Contratação de empresa especializada para o fornecimento de solução como serviço para auditoria, gestão, automação, monitoração e delegação do g
(Microsoft Active Directory), credenciais e perfis de acesso, serviço de diretório local e em nuvem, correio eletrônico local e em nuvem, contemplando o monitoramento de usuá
desvios de comportamento além de permitir delegação de gerenciamento de acesso aos proprietários dos dados, executando ações proativas em múltiplos objetos, identificando e
Incluindo licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, pelo período de 24 meses, renováveis conforme a legislação vigente.

( ) Aquisição de bens _____.
( ) Prestação de Serviço não continuado _____.
( ) Prestação de Serviço continuado SEM dedicação exclusiva de mão de obra _____.
( ) Prestação de Serviço continuado COM dedicação exclusiva de mão de obra _____.
( ) Aquisição de bens e prestação de serviço _____.
(X) A ser definido nos Estudos Técnicos Preliminares

2. JUSTIFICATIVA, NECESSIDADE DA AQUISIÇÃO E RESULTADOS A SEREM ALCANÇADOS

O aumento exponencial de ataques cibernéticos atualmente, faz com que os órgãos da Justiça Eleitoral busquem novas soluções de proteção dos dados, uma vez que esta justiça e
trata, processa e armazena uma grande quantidade de dados e informações diariamente, tanto internamente, como em nuvem, que necessitam ser monitorados, classificados, audi

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 p
contratação de soluções de segurança da informação, com a finalidade mitigar o risco de ataques cibernéticos, e consequentemente elevar o nível de maturidade da gestão da Cibe
Eleitoral..

Portanto, é necessário e urgente o uso de ferramentas e soluções que ofereçam recursos de monitoramento contínuo, detecção, investigação e tratamento de incidentes relacionad
informações institucionais, e que promovam a eficiência no provimento de um ambiente computacional aderente aos controles de segurança da informação, a luz das melhores pr
mais utilizados pelo mercado, ISO 27002, CIS Controls V8.0 e Cobit v4.0.

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 bas
semiestruturadas. Além disso, o GARTNER GROUP apresentou um estudo apontando que, em média, para cada 1 TeraByte de arquivos, existem 50.000 (cinquenta mil) pastas.
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 dad
Proteção de dados – LGPD.

Neste contexto, faz-se necessária aquisição de Solução que permita o Controle e Auditoria para servidores de dados não estruturados na rede interna e em nuvem, controladores d
interno e na nuvem, para reduzir a exposição, detectar ameaças, estar em conformidade com clareza e descomplicação. Conforme levantamento realizado pela STIC, diversas inf
distribuídas em pastas (departamentais, setoriais ou individuais) localizadas no Data Center ou na nuvem do Google Workspace, que são acessadas pelos diversos usuários da red
operacionais que geram registros de eventos (logs). O tratamento, correlação, análise e investigação desses registros é muito trabalhoso e na maioria das vezes ineficiente, pois fa
aprimorar a análise, e não proporciona a devida granularidade quando a necessidade de pesquisar para auditar por exemplo, quem, quando, onde e como um dado foi utilizado, m
encaminhado.

Dessa forma, torna-se necessária a gestão mais eficiente dos dados e informações internas e na nuvem, a auditoria do repositório dos usuários e seus e-mails, com o intuito de ton
casos de incidentes de segurança cibernética, ataques de malwares, ransomwares, ou até mesmo a identificação de acessos indevidos de usuários internos mal intencionados. Sem

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 ent
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 tratam

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 gerenciament
Microsoft). O volume de dados custodiados na infraestrutura mantida pelo Tribunal, torna complexa a administração dos dados, principalmente aqueles relacionados com as pern
serviços disponibilizados pelo serviço de autenticação do AD, como também dificulta bastante identificar se determinado usuário deveria ter realmente o nível de permissão que
períodos de tempo, dificultando a atividade de auditoria do ambiente, o que pode resultar em uma exploração bem sucedida, e dados e informações podem ser comprometidos.

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 i
tornando-se ágeis e precisas as demandas relacionadas à segurança do órgão.

Além disso, essa solução está aderente aos achados 2, 3, 4, 5 e 7, conforme relatório final da Coordenadoria de Auditoria Interna - CAUD (1193668), referente ao processo interr
bem como em relação aos achados 2 e 6 do relatório consolidado de Auditoria Integrada da Justiça Eleitoral nº 1/2022 (1325238), referente ao processo interno 0000319-11.2023
para atender às recomendações exaradas pela CAUD, ou seja, colocar a gestão da Cibersegurança no TRE-DF em conformidade com as melhores práticas definidas pelos framew
pela Justiça Eleitoral (CIS Control V8.0, ISO 27002, e Cobit v4.0).

3. PREVISÃO DA DEMANDA NO PLANO ANUAL DE AQUISIÇÕES OU PCSTIC DO TRE-DF

Qual item do PAA? Este projeto não é previsto no PAA, e sim na Estratégia Nacional de Cibersegurança da JE, que está sendo tratado no processo 0006818-45.2022.6.07.8100,

Qual valor constou da Estratégia Nacional de Cibersegurança da JE? R$ 1.500.000,00.

Qual o valor estimado da despesa? R$ 1.500.000,00.

Obs*: Caso o valor estimado seja superior ao previsto no PAA, será necessária consulta à SEPEO/CORF.

4. ALINHAMENTO DA DEMANDA AOS SEGUINTES INSTRUMENTOS DE PLANEJAMENTO, SE APLICÁVEIS (Indicar os macrodesafios e/ou diretrizes ap planejamento):

PLANEJAMENTO ESTRATÉGICO DO PODER JUDICIÁRIO

Na Estratégia Nacional de Cibersegurança - 2021 a 2024 (TSE e TREs), destaca-se:

Eixo Estruturante E4: Serviços Especializados.

Na Estratégia Nacional do Poder Judiciário 2021-2026, destacam-se aderência às seguintes diretrizes:

- Fortalecimento da estratégia administrativa e da governança judiciária;
- Fortalecimento da relação institucional do Judiciário com a sociedade.

Dentre os objetivos da Resolução 370/2021 CNJ, pode-se destacar:

• Objetivo 2: Promover a Transformação Digital;
• Objetivo 7: Aprimorar a Segurança da Informação e a Gestão de Dados;
• Objetivo 8: Promover Serviços de Infraestrutura e Soluções Corporativas.

Dentre os objetivos da Resolução 396/2021 CNJ, que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), destacam-se:

Art. 6º

I – tornar o Judiciário mais seguro e inclusivo no ambiente digital;

II – aumentar a resiliência às ameaças cibernéticas;

III – estabelecer governança de segurança cibernética e fortalecer a gestão e coordenação integrada de ações de segurança cibernética nos órgãos do Poder Judiciário;

IV – permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

Art. 9º

I – fortalecer as ações de governança cibernética;

II – elevar o nível de segurança das infraestruturas críticas.

Art. 11

I – estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua pre
cada órgão;

IV – utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permit
segurança e oferecer inteligência à análise de eventos de segurança;

PLANEJAMENTO ESTRATÉGICO INSTITUCIONAL DO TRE-DF (PEI)

Macrodesafio: Fortalecimento da Estratégia Nacional de TIC e de Proteção de dados - ID ODS de alinhamento: IX

PLANEJAMENTO ESTRATÉGICO DE STIC DO TRE-DF (PETIC)

Promover Serviços de Infraestrutura e Soluções Corporativas - ID KR1-8.1 (Key-Results);

Aprimorar a Segurança da Informação e a Gestão de Dados - ID KR1-7.1 e 7.2.

PLANO DE GESTÃO DO TRE-DF

Não se aplica

PLANO DE OBRAS DO TRE-DF

Não se aplica

5. QUANTIDADE DO OBJETO E RESPECTIVOS VALORES ESTIMADOS:

Inicialmente está prevista a contratação de empresa especializada para o fornecimento de solução como serviço para auditoria, gestão, automação, monitoração e delegação
AD (Microsoft Active Directory), credenciais e perfis de acesso, serviço de diretório local e em nuvem, correio eletrônico local e em nuvem, contemplando o monitoramen
identificando desvios de comportamento além de permitir delegação de gerenciamento de acesso aos proprietários dos dados, executando ações proativas em múltiplos obj
conteúdos sensíveis. Incluindo licenciamento, instalação, treinamento, garantia e suporte técnico para a solução, pelo período de 24 meses, renováveis conforme a legislaçã

O modelo de contratação será definido no Estudo Técnico Preliminar - ETP.

O custo total estimado para solução foi de R$ 1.500.000,00.

A vigência da contratação à princípio, será de 24 meses, mas será validado no ETP.

6. PREVISÃO DE DATA PARA INÍCIO DA PRESTAÇÃO DOS SERVIÇOS E/OU ENTREGA DO BEM, COM JUSTIFICATIVAS SE HOUVER URGÊNCIA

A entrega da solução deverá ocorrer até o final de Agosto/2023, devendo ser implementada e estar totalmente operacional até Dezembro/2023.

7. VERIFICAR A VIABILIDADE DA REUNIÃO DA DEMANDA PARA AQUISIÇÃO EM CONJUNTO COM OUTRA(S) PREVISTA(S) NO PAA, INCLUSIVE UNIDADES

Por se tratar de solução de tecnologia específica para atendimento de demanda relacionada à gestão da Cibersegurança, não se vislumbra a possibilidade de aquisição em conjunt

8. INFORMAÇÃO ACERCA DA COMPLEXIDADE DA CONTRATAÇÃO

i) COMPLEXIDADE ELABORAÇÃO TR (A) **B**-Baixa, **M**-Média, **A**-Alta
ii) DIFICULDADE EM CONTRATAR (A) **B**-Baixa, **M**-Média, **A**-Alta
iii) RISCO PELA NÃO CONTRATAÇÃO (A) **B**-Baixa, **M**-Média, **A**-Alta

DATA LIMITE CONTRATAÇÃO: 30/08/2023
DATA LIMITE FINALIZAÇÃO TR/PB: 31/05/2023

Obs1: Classificar a complexidade da demanda de acordo com os critérios definidos no artigo 8º da Portaria Presidência nº 130/2018;
Obs2: Definir os prazos limites de contratação e finalização do TR/PB de acordo com o Plano Anual de Aquisições do TRE/DF.

9. INDICAÇÃO DE SERVIDORES PARA COMPOR A EQUIPE DE PLANEJAMENTO DA AQUISIÇÃO

*Mínimo de 2 (dois) servidores e, para STIC, 3 (três), que poderão ser de outras unidades e Secretarias.

Integrante Demandante: Ricardo Negrão de Oliveira - Técnico Judiciário - Matrícula: 0583

Integrante Administrativo: José Fernando Valim Batelli - Técnico Judiciário - Matrícula: 0538

Integrante(s) Técnico(s): Marcelo Nogueira Lino - Técnico Judiciário - Matrícula: 2409

Além dos indicados acima, é importante/necessária a participação de servidores de outras Secretarias ou Unidades na Equipe de Planejamento? ( ) SIM (x) NÃO

Qual Secretaria ou Unidade? Não se aplica

10. IDENTIFICAÇÃO DA ÁREA DEMANDANTE

Unidade/Setor: COIE - Coordenadoria de Infraestrutura

Responsável pela demanda:	Ricardo Negrão de Oliveira	**Matrícula:**	0583

(Assinatura Eletrônica no SEI)

(José Fernando Valim Batelli)

(Coordenador COIE Substituto)

Documento assinado eletronicamente por **JOSÉ FERNANDO VALIM BATELLI**, **Chefe de Seção**, em 17/01/2023, às 14:48, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-df.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1326951** e o código CRC **B8ED5E32**.