TRIBUNAL REGIONAL ELEITORAL DO PARA

Rua João Diogo 288 - Bairro Campina - CEP 66015-902 - Belém - PA

ESTUDOS TÉCNICOS PRELIMINARES

(ETP COMPRAS)

1. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO (obrigatório)

Fundamentação: Descrição da necessidade da contratação, considerado o problema a ser resolvido sob a perspectiva do interesse público (inciso I do § 1° do art. 18 da Lei 14.133/2021 e art. 9°, inciso I da IN 58/2022).

Contratação de solução de detecção e resposta a incidentes, auditoria e proteção de dados, detecção e resposta a ameaças baseadas em dados, coleta fluxos de metadados, e analise constante de dados e de seus repositórios de dados corporativos, plataforma de compartilhamento colaborativo do TRIBUNAL REGIONAL ELEITORAL DO PARÁ - TRE/PA e TRIBUNAIS ELEITOAIS PARTÍCIPES, incluindo prestação de serviço de instalação e configuração, com garantia técnica de 24 (vinte e quatro) meses, com treinamento para capacitação de técnicos do tribunal e serviço de operação assistida e apoio operacional.

1.1. Descrição da demanda

Trata-se de demanda de contratação que tem por objeto a modernização da segurança cibernética dos Tribunais Regionais Eleitorais, cuja solução deve ser baseada em software de auditoria de dados, monitoramento, automação e controle em ambiente on premise Microsoft e ambiente de colaboração em nuvem (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) , devendo compreender o serviço de instalação/configuração, transferência de conhecimento na forma de treinamento oficial, garantia da solução pelo tempo da contratação com atualização/suporte técnico e serviço de técnico operacional na modalidade de operação assistida. O objeto da contratação visa apoiar as equipes de segurança nas atividades de investigação e análise de alertas dos comportamentos suspeitos na Rede interna e ambiente de colaboração em nuvem.

Cumpre salientar que a contratação em questão diz respeito a Licenciamento de software e serviços agregados (Item 1, Anexo I da IN SGD nº 94/2022) e que não incide nas hipóteses vedadas pelo art. 8º da Resolução CNJ nº 468/2022 e pelos artigos 3º e 4º da IN SGD nº 94/2022.

Portanto, tendo em vista a proteção de dados, bem como a inspeção de atividades e gestão de identidades digitais e acessos no ambiente do Active Directory (AD), faz-se necessário a contratação de plataforma de segurança de dados que ofereça recursos avançados para classificar e proteger as informações confidenciais da organização, capaz de prover as seguintes características mínimas desejáveis:

- *Visualização de dados, devendo oferecer uma interface gráfica intuitiva que permita aos usuários administradores visualizar de forma clara o acesso aos dados e as atividades dos usuários. Isso facilita a identificação de ameaças e permite adotar medidas imediatas para proteger as informações custodiadas.*
- *Aumentar a visibilidade e do entendimento do ambiente de TI, permitindo analisar o comportamento dos usuários e de objetos (como permissões, arquivos, metadados, dados não estruturados), auxiliando na identificação de padrões de uso, anomalias, áreas de risco e pontos de vulnerabilidade, permitindo uma melhor compreensão do cenário de segurança cibernética e orientando a implementação de medidas de proteção mais efetivas.*
- *Identificação de ameaças avançadas, por meio da análise de logs, eventos e atividades de usuários em busca de padrões e indicadores de comprometimento. Deve prover técnicas de análise comportamental e algoritmos de machine learning para identificar atividades que podem indicar a presença de ameaças avançadas, como ataques persistentes e furtivos.*

1.2. Identificação das necessidades de negócio e tecnológicas

ID	NECESSIDADES DE NEGÓCIO
1	**Trilha de auditoria** *A solução deve proporcionar a criação de trilhas de auditoria detalhadas capazes de rastrear todas as atividades relacionadas aos dados monitorados, incluindo alterações de permissões, movimentação de arquivos e acesso não autorizado; assim como a atividade de usuários do Active Directory. Essa trilha de auditoria é essencial para fornecer evidências confiáveis sobre as ações realizadas nos dados durante o procedimento de coleta e preservação de evidências.*
2	**Relatórios e documentação** *O software deve gerar relatórios gerenciais detalhados sobre as atividades de usuários bem como sobre o acesso e uso dos dados, bem como sobre as alterações de permissões e configurações. Esses relatórios podem ser utilizados para documentar as evidências coletadas, facilitando a sua apresentação em processos legais e garantindo a rastreabilidade das ações realizadas durante o procedimento.* *A Solução deve possuir a capacidade de gerar insights acionáveis por meio de análises de relatórios. Com base nos dados coletados e analisados, a solução deve possibilitar a identificação de lacunas de segurança, fornecendo recomendações para melhorar a postura e mitigar riscos de segurança da organização, auxiliando na tomada de decisões relacionadas à proteção de dados.*
3	**Auxiliar no Gerenciamento de Crises Cibernéticas** *Através de recursos de análise comportamental e algoritmos de machine learning, o objeto da contratação deve oferecer recursos de identificação de comportamentos suspeitos e atividades maliciosas, permitindo uma detecção precoce de ameaças. Além disso, deve ainda apoiar as equipes em atividades de resposta a incidentes e auxiliar auditoria e conformidade regulatória. De modo geral, deve capacitar as organizações a tomar medidas rápidas e eficazes para lidar com crises cibernéticas e minimizar os impactos dos ataques à infraestrutura de segurança.*
4	**Monitoramento de atividades e dados não estruturados** *O software deve monitorar as atividades de acesso e uso dos dados em tempo real, registrando todas as ações realizadas pelos usuários. Isso inclui informações como quem acessou, quando acessou, quais arquivos foram visualizados, modificados ou copiados, entre outros detalhes. Esses registros podem ser usados como evidências para investigações e auditorias do órgão.* *Deve possuir capacidade de monitoramento de dados não estruturados. Os dados não estruturados são informações que não seguem um formato predefinido, como documentos, arquivos de texto, planilhas, apresentações, e-mails, registros de logs, entre outros. Esses dados*

	são geralmente mais difíceis de gerenciar e proteger devido ao volume de arquivos e distribuição em diversos locais, on premise ou em nuvem.
5	**Possuir conformidade com regulamentações existentes** *Deve ser capaz de auxiliar na aderência de regulamentações associadas a privacidade e proteção de dados, como a Lei nº 13.709/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD); a Resolução CNJ nº 396, de 7 de junho de 2021 - institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ); as Normas Internacionais de Segurança da Informação (ISO 27001/27002/*27005/22301*) e CIS Control V.8 (Critical Security Controls), dentre outras.*

ID	NECESSIDADES TECNOLÓGICAS
1	**Inteligência Artificial (IA)** *O software deve incorporar recursos de inteligência artificial (IA) objetivando aprimorar as funcionalidades de análise e proteção de dados. Esses recursos de IA devem incluir a identificação de padrões, comportamentos e anomalias nos dados e comportamentos registrados dos usuários, fornecendo insights que possibilitem a detecção avançada de ameaças.* *A IA deve ser utilizada pelo órgão para melhorar sua capacidade de classificação de dados e identificação de informações confidenciais, possuindo a capacidade de reconhecer automaticamente tipos de arquivos, atribuir níveis de sensibilidade e aplicar políticas de proteção adequadas aos dados identificados. Isso ajuda a simplificar o processo de classificação e aprimora a eficiência na proteção de dados sensíveis.*
2	**A análise comportamental** *Deve utilizar algoritmos de aprendizado de máquina para entender o comportamento padrão dos usuários e identificar atividades anômalas que possam indicar ações suspeitas ou maliciosos. Ele pode detectar tentativas de acesso não autorizado, uso indevido de informações confidenciais, violações de políticas de segurança e outros eventos relevantes, permitindo a adoção de medidas preventivas e corretivas, antes que ocorram violações de dados.*
3	**Identificação e classificação de dados** *Auxiliar na identificação e classificação os dados em sistemas de arquivos armazenados em servidores locais ou em nuvem; incluindo arquivos, documentos e informações sensíveis. Objetiva facilitar a seleção e o isolamento das evidências relevantes para o procedimento de visibilidade de dados não estruturados, garantindo que as informações críticas do órgão sejam conhecidas e preservadas.*
4	**Identificação de alterações não autorizadas** *O software deve identificar alterações não autorizadas nos arquivos e nas permissões de acesso, ajudando a detectar possíveis tentativas de adulteração ou destruição de evidências. Isso é fundamental para garantir a integridade das evidências coletadas.*
5	**Detalhes sobre as necessidades tecnológicas mínimas da solução** A solução deve possuir as seguintes funcionalidades: • Simplificar operações em lote de múltiplos objetos no AD, em servidores de arquivos ou no correio eletrônico. • Automatizar tarefas repetitivas, comuns ou complexas, associadas ao gerenciamento do AD. • Analisar o ambiente, coletar informações sobre objetos, arquivos e caixas de correio. • Gerar relatórios que permitam garantir a efetividade de controles de segurança, assim como uma visão do estado atual e histórico de usuários e acessos. • Permitir responder quem, quando, onde e como um determinado objeto foi acessado, editado ou excluído. • Permitir a identificação de tentativas ou acessos, aceitos ou rejeitados, de usuários, computadores ou sistemas. • Permitir identificar a frequência de utilização e o último acesso aos objetos e arquivos auditados. • Permitir identificar permissões de acesso ou de modificação não necessárias aos recursos, arquivos ou caixas de correio. • Permitir identificar a origem dos acessos a arquivos e objetos. • Permitir o acesso às informações de auditoria em tempo real ou em histórico de, no mínimo, 5 anos. • Permitir automatizar a identificação, a remoção de permissões, a desativação e a remoção de objetos e arquivos com base em informações de auditoria. • Detectar atividades não autorizadas de processamento de informações. • Permitir a configuração de alertas com base nas informações auditadas. • Permitir a auditoria de informações de acessos tanto de administradores quanto dos usuários dos serviços. • Utilizar de forma eficiente o espaço em disco necessário para armazenamento dos eventos de auditoria. • Utilizar as informações auditadas para sugerir melhorias no uso dos recursos. • Permitir a gestão eficiente dos recursos auditados. • Permitir a identificação e classificação de conteúdos sensíveis em servidores de arquivos. • Permitir a identificação dos proprietários dos dados, listas de distribuição e caixas de correio individuais ou corporativas. • Monitorar os eventos das caixas postais dos usuários e das pastas públicas. • A coleta de informações de auditoria não deve onerar o processamento nos servidores alvo. • Permitir o ajuste os diretórios com herança quebrada de permissões. • Assegurar que as autorizações são baseadas em necessidades de negócio. • Suportar a versão atual e posteriores do Active Directory, do correio eletrônico e do serviços de arquivos (versões atuais dos sistemas operacionais: Windows Server 2016 ou superior) • Permitir auditar contas de usuários. • Permitir auditar contas de usuários/sistemas. • Permitir auditar grupos do AD. • Permitir auditar objetos de computadores do AD. • Permitir auditar objetos diversos do AD. • Permitir auditar servidores de arquivos existentes no ambiente da Justiça Eleitoral. • Permitir auditar servidores do Microsoft Exchange • Permitir auditar caixas de correio eletrônico. • Suportar a utilização de servidores virtualizados para todos os seus componentes. • Monitorar diferentes domínios, independente da existência de relação de confiança. • Gerar relatórios de todas as consultas e ações feitas pelos usuários através da interface gráfica da solução, de modo que também seja possível realizar auditoria. • Permitir descoberta e classificação de dados sensíveis e trilha de auditoria de acesso dos usuários aos dados armazenados em nuvem corporativa Microsoft, Google ou AWS. • Deverá demonstrar dados sensíveis compartilhados externamente e expostos publicamente.

- Deverá apresentar métricas e configurações incorretas que podem afetar a segurança do ambiente, como: pastas e repositórios expostos publicamente, dados inativos.

1.3. Motivo/Justificativa da Contratação

O cenário do Poder Judiciário Brasileiro configura atualmente um processo acelerado de transformação digital, no qual as soluções tecnológicas que possibilitam o tratamento de dados se tornam imprescindíveis para uma prestação jurisdicional mais efetiva. A efetividade do referido processo só ocorrerá com a devida e correspondente proteção de dados, informações e usuários.

Neste cenário, ventos recentes de ataques cibernéticos a alguns órgãos do Poder Judiciário descortinam um horizonte de ameaças que põe em risco o aludido planejamento, cujos incidentes demonstram o poder desses atacantes e a necessidade cada vez maior de implementar ações preventivas, detectivas e corretivas, de forma estruturada, objetivando antecipar incidentes e mitigar os impactos de ataques cibernéticos.

No Brasil, a escalada de ataques cibernéticos motivou a cúpula do Poder Judiciário, por meio do CNJ, a criar o Comitê de Segurança Cibernética do Poder Judiciário, via Publicação da Portaria CNJ Nº 242 de 10/11/2020 (CNJ, 2020). Os normativos publicados pelo Conselho Nacional de Justiça, como a Resolução CNJ N° 396/2021 e Portaria CNJ nº 162/2021, impõem uma série de novas responsabilidades e um conjunto inexplorado de boas práticas e atividades técnicas que teriam o objetivo de estabelecer um novo ecossistema de segurança cibernética para os Órgãos do Poder Judiciário.

De outro lado, a Resolução TSE nº 23.644/2021, que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral, instituiu como princípio norteador a garantia da disponibilidade, integridade, confidencialidade, autenticidade, irretratabilidade e audibilidade das informações produzidas, recebidas, armazenadas, tratadas ou transmitidas pelos órgãos da Justiça Eleitoral, no exercício de suas atividades e funções. Deste modo, o conjunto de orientações que fundamentam a Resolução TSE nº 23.644/2021 estão em consonância com o objetivo dessa contratação.

Nestes termos, a atenção relativa à segurança deve ser dispensada não somente aos sistemas informatizados, mas também aos ativos que recebem, processam, armazenam, publicam e descartam informações. Na sociedade da informação vivida nos tempos atuais, ao mesmo tempo em que as informações são consideradas o principal patrimônio de uma organização, estão estas sob constantes ameaças e necessitam ser adequadamente protegidas. Com isso, a Segurança da Informação tornou-se essencial ao funcionamento de empresas privadas e órgãos públicos, visando a continuidade da entrega de serviços, sobrevivência e credibilidade das instituições.

Por este motivo, além do risco de perda e vazamento de dados sensíveis durante ataques cibernéticos, existe a preocupação de que a sociedade perca a confiança nos serviços disponibilizados, entre outras inúmeras consequências à imagem do Tribunal. Para que seja alcançado o nível de segurança exigido atualmente, é necessário investir em processos, sistemas e conhecimento específicos contra ameaças avançadas.

Neste contexto, a Secretaria de Tecnologia da Informação - STI do Tribunal Regional Eleitoral do Pará entende ser necessária a contratação de serviços e soluções de tecnológicas de segurança da informação cuja eficiência na mitigação de ataques cibernéticos seja comprovada e que permitam o provimento eficiente da integração entre todos os recursos necessários à auditoria e mitigação dos riscos sistêmicos de segurança cibernética, contando com atividades contínuas e especializadas em alerta, tratamento e mitigação de eventos e incidentes de segurança.

A necessidade da contratação proposta possui amparo legal na Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), que apontou a necessidade de contratação e implantação de solução de segurança - Monitoração e auditoria de E-mail, arquivos e AD. De igual forma, esta ação está em consonância com o Plano Diretor de Tecnologia da Informação - PDTI STI/TRE-PA 2023/2024 (IN SGD nº 94/2022, art. 6º, I), URL:

- https://www.tre-pa.jus.br/institucional/governanca-institucional/governanca-de-ti-1/arquivos-governanca-de-ti/p-lano-diretor-de-tecnologia-da-informacao-pdti-2023 (página 16)

A pretensa contratação tem como objetivo principal, transformar de forma positiva a maneira como a prevenção de ataques cibernéticos é gerenciada pelas unidades de defesa cibernética da STI, garantindo a complementação efetiva dos controles já utilizados, visando prover soluções de inspeção e proteção contra ameaçadas avançadas nos servidores de Diretórios (AD), dispositivos de armazenamento local e em nuvem, bem como aprimorar a proteção e resiliência dos serviços tecnológicos ofertados pelo Tribunal.

2. REQUISITOS DA CONTRATAÇÃO

Fundamentação: descrição dos requisitos da contratação necessários e suficientes à escolha da solução, prevendo critérios e práticas de sustentabilidade, observadas as leis ou regulamentações específicas, bem como padrões mínimos de qualidade e desempenho (inciso III do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso II da IN 58/2022).

2.1. Natureza do objeto:

Objeto da contratação é considerado comum, associado ao fornecimento de licenças de software pronto, bem como serviços associados à implantação e treinamento da solução. Nestes sentido, a solução apresenta padrões de desempenho e de qualidade que podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

2.2. Necessidade continuada do fornecimento:

O objeto da contratação se estende necessariamente por mais de um ano?

(X) SIM ( ) NÃO

Justificativa: os serviços de garantia e suporte técnicos das soluções de segurança cibernética se estendem por mais de um ano, pois são necessários para a diminuição da superfície de ataques, mitigação de riscos cibernéticos e proteção de dados informatizados do Tribunal, o que caracteriza a sua natureza continuada.

O objeto da contratação é essencial para a continuidade do negócio?

(X) SIM ( ) NÃO

Justificativa: o fornecimento de bens e serviços é enquadrado como continuado tendo em vista a necessidade permanente (ou prolongada) para manutenção da atividade administrativa do órgão de garantia da segurança cibernética, sendo a vigência plurianual mais vantajosa considerando as justificativas constantes deste Estudo Técnico Preliminar.

2.3. Forma/regime de execução/fornecimento

A forma de execução será definita em tópico específico deste ETP e no TR.

Na execução do contrato será adotado o regime de empreitada por preço unitário.

O certame se realizará na modalidade Pregão, na forma eletrônica, para formação de registro de preços, cujo critério de julgamento será o de menor preço global.

2.4 Adoção da sistemática do registro de preços

2.4.1. Será adotado o Sistema de Registro de Preços – SRP? Caso positivo, justificar.

(X) Sim ( ) Não

Justificativa: Lei 14.133/2021, art. 3º do Decreto 11.462/2023, inciso III - quando for conveniente para atendimento a mais de um órgão ou a mais de uma entidade, inclusive nas compras centralizadas. Deste modo, a contratação visa atender a Estratégia Nacional de Cibersecurança TSE e TREs (2021 a 2024) que prevê, por media de economia de escala e padronização de soluções de Segurança adotadas pelos TREs, que as contratações serão feitas sempre de forma conjunta.

2.4.2. Haverá órgãos participantes deste Registro de Preços? Justificar.

(X) Sim ( ) Não ( ) Não se aplica

Justificativa: A contratação conjunta mediante IRP visa atender no Eixo Estruturante E3 - Ferramentas Automatizadas (Ferramentas de Segurança Interna), associado à Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), que apontou a necessidade de contratação e implantação de solução de segurança - Ferramentas de Segurança Interna - Monitoração e auditoria de E-mail, arquivos e AD (por exemplo, Varonis).

2.4.3. Foi realizado procedimento público de intenção de registro de preços - IRP?

(X) Sim ( ) Não; justificativa abaixo ( ) Não se aplica

2.4.3.1. Foi realizada consulta inicial via Ofício-Circular nº 5 / 2023 - TRE-DF/PR/DG/GDG entre os Tribunais Regionais Eleitorais para levantamento de interesse, conforme item 13.1, suprindo o registro da intenção de registro de preços em sistema próprio, considerando tratar-se de contratação associada à Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), portanto, direcionada somente à Justiça Eleitoral.

2.4.3.2. Será realizada nova consulta para consolidação de quantidades referentes aos itens e ratificação da participação na Ata RP.

2.4.4. Foi estabelecido (se for o caso) o número máximo de participantes, em conformidade com a capacidade de gerenciamento do órgão? Justificar.

( ) Sim ( ) Não; justificativa abaixo (X) Não se aplica

Obs: o número máximo de participantes está limitado ao quantitativo de regionais interessados.

2.4.5. Será admitida a adesão à ata de registro de preços por órgão não participante? Justificar.

(X) Sim ( ) Não ( ) Não se aplica

Justificativa: *será permitida a adesão aos Tribunais Regionais Eleitorais que não figuram como partícipes desta Ata de Registro de Preços, em razão da arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).*

Neste sentido, esclareço que a demanda para contratação do objeto, conforme mencionado neste ETP, refere-se às atividades relacionadas a contratações de Soluções de Segurança da Informação previstas na Arquitetura de Cibersegurança (evento 1610000), cujo escopo foi elaborado pelo Grupo de Trabalho de Segurança da Informação (TSE) a partir da Estratégia Nacional de Cibersegurança.

Para tanto, dentre as contratações previstas no Arquivo Arquitetura de Cibersegurança - Anexo_1778310_Anexo_I___Ferramentas___Final_10_09_2021 (evento 1405279), consta a contratação de AUDITORIA DE ARQUIVOS E EMAILS, conforme demonstra o quadro a seguir.

ID	SGT	PID	SOLUÇÃO	REQUISITOS FUNCIONAIS	EXEMPLOS DE MERCADO	CRITICIDADE	ISO 27002:2013	CIS CONTROLS V 7.1	EIXOS
ID_F26	SG13	PID13	AUDITORIA DE ARQUIVOS E EMAILS	AUDITORIA, DLP	VARONIS, NETWRIX, IBM STOREIQ, VERITAS	2	9.2.5, 9.2.6	13.4, 16.7	4,7

Como parte da iniciativa de contratações conjuntas referente à Estratégia Nacional de Cibersegurança (evento 1370070), o TRE-PA e TRE-DF foram designados para coordenação aquisição da solução AUDITORIA DE ARQUIVOS E EMAILS. Deste modo, conforme direcionamento recebido nas reuniões de planejamento realizadas pelo TSE, informo que houve a orientação do STI/TSE para que as contratações fossem realizadas através de Registros de Preços, no qual os itens poderiam ser demandados pelos Tribunais Regionais Eleitorais partícipes da contratação conjunta (vide evento 1370070, pg 14):

> *A Estratégia Nacional, dessa forma, propõe que uma das atribuições da pessoa dedicada à cibersegurança em cada Tribunal seja ajudar o esforço nacional de aquisições, configurações e implantações dessas ferramentas. A proposta compreende a formação de grupos de quatro TREs que deverão, por meio de seu profissional em cibersegurança, escrever (ou adaptar a partir de originais do TSE) as documentações necessárias para a **condução de contratações por meio de ARP, à qual todos os TREs que precisam de referida ferramenta possam aderir**. O TSE apoiará essa iniciativa (mesmo que já tenha a referida ferramenta) compartilhando documentações que possam ser utilizadas como base para as novas contratações.*

Além disso, foi recomendado pelo STI/TSE facultar aos TREs que não figurassem no rol de partícipes a possibilidade de contratação das soluções de segurança por meio de adesão à Ata RP (carona), conforme ocorreu no processo IRP 0008981-46.2021.6.14.8000. A proposta de Ata RP foi justificada, em razão da possibilidade de padronização das soluções contratadas pela JE, evitando, deste modo, aquisições de soluções de diferentes fabricantes. Do ponto de vista técnico, a adoção de soluções diferentes daquelas já adotadas pela JE poderia resultar, consequentemente, na dificuldade de investigações de ilícitos cibernéticos envolvendo mais de um TRE, em razão da complexidade da análise de ferramentas de logs distintas e trilhas de auditorias de diferentes soluções.

Cumpre salientar que a solução demandada é adequada ao ambiente da JE, em razão da similaridade da infraestrutura de rede e Serviços de Diretórios (vide item 13.1 do ETP) existente nos Tribunais.

2.5. Admissão ou não de subcontratação do objeto contratual

( ) SIM (X) NÃO

2.6. Da participação de consórcios, cooperativas e pessoas físicas

2.6.1. Não será permitida a participação de empresas em consórcio, pois a natureza do fornecimento de licenças de software não enseja a necessidade da previsão da formação em consórcio por si, uma vez que o objeto consiste no fornecimento de um produto digital cuja logística não se apresenta como complexa para fornecimento, ou seja, uma única revenda detêm em seu portifólio de serviço condições de atender as demandas prevista neste TR, sem a necessidade de se consorciar com outra empresa para conseguir atender o objeto na sua completude. Desse modo, não há situação fática que comprove a necessidade da previsão do uso do instituto do consórcio no presente processo..

2.6.2. Considerando as características do objeto e agrupamento dos itens, não será permitida a participação de pessoas físicas e cooperativas, pois a presente contratação exige estrutura mínima da contratada, com equipamentos, instalações e equipe de profissionais ou corpo técnico para a execução do objeto, incompatíveis com a natureza profissional da pessoa física (art. 4º da IN SEGES /ME nº 116/2021) e diretrizes previstas no art. 10 da IN Seges nº 05/2017 para a participação de cooperativas.

2.7. Exigência de amostra

(X) SIM ( ) NÃO

2.7.1. Após o aceite da proposta quanto ao valor e havendo dúvidas no tocante ao atendimento das especificações técnicas, o pregoeiro poderá solicitar, primeiramente, catálogo ou documento similar que comprove a conformidade do produto ofertado, devendo o licitante informar o sítio do fabricante;

2.7.2. Inexistindo catálogo ou sendo este insuficiente para análise técnica das especificações do produto, o interessado classificado provisoriamente em primeiro lugar deverá apresentar amostra, na forma de prova de conceito, que terá data, local e horário de sua realização divulgados por mensagem no sistema, cuja presença será facultada a todos os interessados, incluindo os demais fornecedores interessados, mediante solicitação ao pregoeiro, para prévio agendamento com a unidade técnica.

2.7.3. O TR deverá disciplinar a forma como essa etapa ocorrerá, bem como os critérios a serem adotados para a avaliação.

2.8 Garantia, manutenção e assistência técnica

A solução contratada deverá contar com garantia mínima de 24(vinte e quatro) meses, com o objetivo de prover a continuidade das operações, e oferecer suporte técnico e manutenção durante todo o período contratual. A garantia refere-se ao período oficial de suporte da solução, fornecido por seu fabricante, compreendendo o fornecimento de atualizações e correções durante todo o ciclo de vida da solução.

2.9. Garantia contratual

2.9.1 Será exigida a garantia contratual da execução, nos termos do art. 96 da Lei 14.133/2021, a ser devidamente especificada no Termo de Referência, tendo em vista o valor estimado da contratação ser de monta considerável, bem como aos riscos inerentes à solução contratada para o Tribunal, conforme estabelecido na matriz de risco.

2.10. Requisitos de capacitação

2.10.1. A contratação deverá fornecer TREINAMENTO, com carga horária mínima de 20 (vinte) horas, e deverá ser realizado em Belém/PA em turmas fechadas de até 10 participantes com emissão de certificado de participação, sendo que, a critério do CONTRATANTE, poderão ser indicados mais participantes na categoria de ouvintes, sem a exigência de certificado de participação e material (limitando-se a 4 participantes adicionais do tipo "ouvintes"). Considerando que todas as despesas referentes à realização do treinamento ou ao custeio de insumos deverão estar inclusas no preço contratado.

2.11. Requisitos legais e conformidade

- *Resolução Nº 468 de 15/07/2022, Dispõe sobre diretrizes para as contratações de Solução de Tecnologia da Informação e Comunicação pelos órgãos submetidos ao controle administrativo e financeiro do Conselho Nacional de Justiça (CNJ).*
- *Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, Dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISP do Poder Executivo Federal.*
- *Resolução CNJ nº 370/2021, institui a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD).*
- *Resolução CNJ nº 396, de 7 de junho de 2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).*
- *Portaria Nº 162 de 10 de junho de 2021 (e anexos), que aprova Protocolos e Manuais criados pela Resolução CNJ nº 396/2021, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).*
- *Norma Complementar nº 08 /IN01/DSIC/GSIPR - Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.*
- *Norma Complementar nº 21 /IN01/DSIC/GSIPR - Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.*
- *LGPD – Lei Geral de Proteção de Dados (Lei no 13.709/2018), e Marco Civil da Internet Lei no 12.965/2014.*
- *Resolução TSE Nº 23.644, de 1º de julho de 2021, Dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral.*
- *Lei Nº 14.133, de 1º de abril de 2021, Nova Lei de Licitações e Contratos, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, Estados, Distrito Federal e Munícipios.*
- *Decreto nº 11.462, de 31 de março de 2023. Regulamenta os art. 82 a art. 86 da Lei nº 14.133, de 1º de abril de 2021, para dispor sobre o sistema de registro de preços para a contratação de bens e serviços, inclusive obras e serviços de engenharia, no âmbito da Administração Pública federal direta, autárquica e fundacional.*
- *Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024).*

Deverão ser observadas, no que se aplicar, as boas práticas de mercado conforme estabelecido nos padrões e metodologias descritas a seguir:

- *NBR ISO/IEC n° 27001:2013 (Sistemas de gestão da segurança da informação — Requisitos);*
- *NBR ISO/IEC n° 27002:2013 (Código de prática para controles de segurança da informação);*
- *NBR ISO/IEC n° 22301:2020 (Segurança da sociedade — Sistema de gestão de continuidade de negócios — Requisitos);*
- *NBR ISO/IEC n° 27005:2019 (Gestão de riscos de segurança da informação); e*
- *NBR ISO/IEC n° 31000:2018 (Gestão de riscos – Diretrizes).*

A solução a ser contratada deve ainda atender a conformidade de normas ISO relacionadas à segurança da informação, dentre elas:

- ISO 27001: Esta norma estabelece requisitos para um Sistema de Gestão de Segurança da Informação (SGSI) e fornece diretrizes para a implementação de controles de segurança adequados. O objeto da contratação deve oferecer recursos que possibilitem o atendimento aos requisitos da ISO 27001, como a detecção de violações de acesso, controle de permissões, monitoramento de atividades e análise de riscos.
- ISO 27002: Essa norma ISO fornece diretrizes para implementação de controles de segurança da informação. O objeto da contratação deve auxiliar na implementar controles de segurança recomendados pela ISO 27002, como a classificação de dados, a auditoria e monitoramento de eventos, a gestão

de identidades e acessos, entre outros.

- ISO 27005: Esta norma trata da gestão de riscos de segurança da informação. O objeto da contratação de oferecer recursos de análise de riscos, como a identificação de atividades suspeitas, análise de comportamento, detecção de ameaças internas e recomendações de permissões de acesso, que auxiliam na implementação de uma abordagem de gerenciamento de riscos eficaz.
- ISO 22301: A norma 22301 é específica para a gestão de continuidade de negócios. Embora o objeto da contratação possua como principal foco a segurança da informação, os recursos de monitoramento, detecção de ameaças e análise comportamental esperados na aludida solução podem contribuir indiretamente para a resiliência e continuidade dos negócios, fornecendo informações valiosas para a tomada de decisões relacionadas à continuidade operacional e gestão de incidentes cibernéticos.

2.12. Requisitos de Segurança da Informação

- A Contratada deverá submeter-se aos procedimentos de segurança existentes no órgão, ou que possam ser criados durante a vigência do contrato. Os procedimentos deverão ser observados sempre que for necessária o acesso presencial ou remoto à infraestrutura da Contratante.
- A empresa contratada deverá respeitar as diretrizes constantes da **Política de Segurança da Informação do da Justiça Eleitoral** (Resolução TSE Nº 23.644, de 1º de julho de 2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Pará, e de outros partícipes desta contratação, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.
- O Tribunal Regional Eleitoral do Pará terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.
- Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).
- O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e proteger todos os dados de infraestrutura e de vulnerabilidades do contratante a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.
- Informações a que a CONTRATADA terá acesso deverão ser utilizadas somente nos processos envolvidos para execução do objeto contratado.
- A solução deverá proporcionar a disponibilidade, a integridade e a segurança de todas as informações do TRE-PA por ela gerenciadas e armazenadas.
- Solução deve apresentar conformidade com a Lei Geral de Proteção de Dados – LGPD.
- O Tribunal deverá adotar precauções e medidas para que as obrigações oriundas do presente instrumento sejam efetivamente observadas a todos os seus representantes.
- A CONTRATADA deverá informar imediatamente ao TRE qualquer violação das regras de sigilo ora estabelecidas que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo, bem como de seus empregados, prepostos e prestadores de serviço.

2.13. Requisitos ambientais, sociais e culturais

- Os softwares aplicativos e interface do software devem ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.
- Visando a inclusão social, a solução deverá possuir um modo de operação para pessoas com dificuldade ou incapacidade de diferenciar cores.
- Quanto aos requisitos sociais, os profissionais da CONTRATADA, quando nas dependências do TRE-PA, deverão apresentar-se com crachá de identificação, vestidos de forma adequada ao ambiente de trabalho, evitando-se o vestuário que caracterize o comprometimento da boa imagem institucional.

2.14. Requisitos temporais

- Todos os eventos de trabalho que envolva participação de integrantes do TRE-PA serão realizados de segunda-feira a sexta-feira das 08:00 às 17:00, exceto feriados, salvo casos de urgência e/ou acordo entre as partes.
- Todos os eventos de trabalho que envolva participação de integrantes da CONTRATADA em ambiente da CONTRATANTE serão realizadas de segunda-feira a sexta-feira das 08:00 às 17:00, exceto feriados, salvo casos de urgência e/ou acordo entre as partes.
- Não será computado o tempo de atraso quando este estiver sido ocasionado pela CONTRATANTE ou por fatos supervenientes que independam de ações da CONTRATADA, desde que devidamente justificado e aceito pela CONTRATANTE.
- Não são considerados casos ou fatos supervenientes as situações externas que poderiam ter sido contornadas ou mitigadas por ações de logísticas preventivas ou reativas da CONTRATADA.

Fases associadas à execução do objeto: As fases e prazos referentes à execução objeto estão consolidados na tabela a seguir:

ITEM	DESCRIÇÃO	PRODUTOS FINAIS A SEREM ENTREGUES	PRAZO DA ENTREGA
1	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇAS DE SOFTWARE	30 dias corridos, contados do recebimento da ordem de fornecimento.
2	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇAS DE SOFTWARE	30 dias corridos, contados do recebimento da ordem de fornecimento.
3	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇAS DE SOFTWARE	30 dias corridos, contados do recebimento da ordem de fornecimento.
4	SERVIÇO DE INSTALAÇÃO, IMPLANTAÇÃO, PARAMETRIZAÇÃO E OPERACIONALIZAÇÃO (PARCELA ÚNICA)	AMBIENTE IMPLANTADO E CONFIGURADO	30 dias corridos, contados do recebimento da ordem de serviço. Obs. Esse prazo compreende as fases de abertura e planejamento descritas no

			item 3.4.1 da especificação do objeto.
5	TREINAMENTO OFICIAL, NA FORMA REMOTA (ONLINE), COM DURAÇÃO DE 20 HORAS, PARA ATÉ 10 PARTICIPANTES (PARCELA ÚNICA)	SERVIÇO / TREINAMENTO	45 dias corridos, contados do recebimento da ordem de serviço
6	SERVIÇO DE APOIO OPERACIONAL, INVESTIGAÇÃO E ANÁLISE DE ALERTAS E COMPORTAMENTOS SUSPEITOS, COM PAGAMENTO MENSAL.	SERVIÇO DE APOIO OPERACIONAL	Disponibilização do serviço, no dia útil posterior à emissão e assinatura do Termo de Recebimento Definitivo (TRD) da solução pela CONTRATANTE.

Tabela - Fases e prazos referentes à execução objeto

2.15. Dinâmica de execução do contrato

1. O Modelo de Execução do Contrato definirá como o contrato deverá produzir os resultados pretendidos desde o seu início até o seu encerramento.
2. Fixação das rotinas de execução.
    a. Os serviços contratados deverão ser executados pela CONTRATADA em dias úteis e em horários de expediente regulares, entre às 08:00 e12:00h e13:00 e 17:00 horas. Em caso em que haja algum impedimento para a execução normal dos serviços ou que possam comprometer o funcionamento das unidades administrativas, a fiscalização poderá determinar a CONTRATADA à execução em horários alheios ao expediente, em feriados ou finais de semana, sem qualquer ônus extras ao Contratante.
    b. Os bens deverão ser entregues no endereço do Contratante designado no instrumento contratual, de segunda a sexta-feira, no horário das 08 às 15h, ou em outro horário definido pela fiscalização do contrato.
    c. Caso não seja possível a entrega dos itens na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10(dez) dias úteis de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.
3. Forma de pagamento. O pagamento dos produtos e serviços que compõe o objeto ocorrerá na forma estabelecida no Termo de Referência, de acordo com o tipo de objeto, após o recebimento definitivo, efetuado em função dos resultados obtidos.
    a. A Contratada só poderá emitir as Notas Fiscais mediante a emissão de cada relatório de execução do objeto. Após o recebimento de cada Nota Fiscal, a Contratante efetuará o pagamento à Contratada em até 10 (dez) dias.
    b. O valor total dos serviços, incluindo todos os impostos, taxas e as despesas referentes à execução das atividades, deverá estar incluso na proposta comercial.
4. Mecanismos formais de comunicação. A comunicação entre a CONTRATANTE e a CONTRATADA se dará, preferencialmente, por meio escrito, sempre que se entender necessário o registro de ocorrência relacionada com a execução do contrato. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:
    a. Ordem de Fornecimento de Bens e Serviços;
    b. Ata de Reunião;
    c. Ofício(s);
    d. Sistema de abertura de chamados da CONTRATADA;
    e. E-mails e Notificações Administrativas;
    f. Reuniões de *kick off* poderão ser exigidas pela Fiscalização, sem ônus algum para o TRE-PA.
5. Deverão ser previstos os seguintes documentos contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade.
    a. Termo de Compromisso, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes no órgão ou entidade, a ser assinado pelo representante legal da contratada; e
    b. Termo de Ciência da declaração de manutenção de sigilo e das normas de segurança vigentes no órgão ou entidade, a ser assinado por todos os empregados da contratada diretamente envolvidos na contratação.
6. O Modelo de Execução do Contrato foi elaborado com base nas exigências do art. 18 da IN SGD nº 94/2022.

2.16. Dos prazos

2.16.1. A contagem dos prazos referente a entrega de produtos e serviços será em dias corridos, conforme período consignado em cada etapa.

2.16.2. A contagem dos prazos de entrega pelo contratado será iniciada na data de confirmação do recebimento da ordem de serviço correspondente à etapa.

2.16.3. Os prazos de entrega, substituição e reposição admitem prorrogação quando houver motivos justificáveis e devidamente fundamentados, como a ocorrência de casos fortuitos ou de força maior, impossibilidade de cumprimento do prazo por motivos técnicos ou circunstâncias imprevisíveis, entre outros. No entanto, cumpre destacar que o(s) pedido(s) de prorrogação devem ser encaminhados para a fiscalização do contrato, pelo menos, 10(dez) dias antes de encerramento do(s) prazo(s), para análise e parecer da Administração.

2.16.4. O prazo de vigência da contratação é de 24 (vinte e quatro meses) meses contados da data de assinatura do contrato, prorrogável, caso necessário, por até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

2.16.5. O término da vigência do contrato não exonera a CONTRATADA de sua responsabilidade em promover e assegurar a assistência técnica da garantia, estando sujeita, na hipótese do descumprimento da responsabilidade assumida e mesmo depois de expirada a vigência do contrato, às penalidades previstas neste Termo de Referência, sem prejuízo de eventual responsabilidade civil e penal.

2.17. Critérios e práticas de sustentabilidade

Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:

2.17.1. Todos os manuais, guias de instruções e ajuda deverão ser disponibilizados preferencialmente para o idioma Português do Brasil - PtBR e fornecidos em meio digital;

2.17.2. Não empregar menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

2.17.3. Não possuir empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

2.17.4. Cumprir as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas.

2.18. Requisitos de qualificação técnica ou econômica

2.18.1. A licitante deverá apresentar, como condição de habilitação (qualificação técnico operacional), aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

2.18.2. O atestado de capacidade ou qualificação técnica é o documento que se destina à comprovação de aptidão para o fornecimento de bens e serviços similares de complexidade tecnológica e operacional equivalente ou superior com o objeto da contratação. Em linhas gerais, este documento tem por objetivo demonstrar que a licitante proponente já atuou no mercado executando atividade pertinente e proporcional com o objeto da licitação, e/ou forneceu em contratos anteriores produtos com qualidade, capacidade, aparelhamento necessário para a implantação almejada. De outro lado, a qualificação técnica também serve para demonstrar a expertise da equipe técnica que se responsabilizará pelos serviços que a administração pública deseja contratar.

2.18.3. A exigência de qualificação técnica para a aludida contratação, possui como finalidade comprovar que o licitante possui aptidão operacional necessária para a realização da atividade pertinente ao objeto da licitação e, quando for o caso, o conhecimento técnico especializado e a capacitação operativa para cumprir o objeto do contrato, tendo em vista a especificidade e complexidade do objeto. (Art. 67, da Lei nº 14.133/2021).

2.18.4. Destarte, pelos motivos supracitados, pode-se inferir que é primordial a experiência técnica das licitantes para a contratação em tela. Pensar de maneira diferente, permitindo que empresas e profissionais sem nenhuma experiência anterior na elaboração de projetos similares participem desse certame, significaria prestigiar a imprudência e negligência do interesse público. Logo, deverá ser exigida a qualificação técnica.

Nesse contexto, a inclusão do atestado de capacidade técnica cumpre as seguintes finalidades:

- Garantia de Qualificação Técnica mínima: visa garantir a qualidade de eficiência dos serviços prestados, bem como a proteção dos interesses públicos, mediante comprovação da experiência prévia do licitante na execução de projetos de complexidade semelhantes. Por se tratar de contratação de subscrição de software, que inclui serviços de instalação e suporte, a qualificação técnica dos licitantes é fundamental para assegurar que possuem a capacidade necessária para implementar e dar suporte efetivo à solução de segurança que será instalado no ambiente do contratante.
- Redução de Riscos: A inclusão do atestado de capacidade técnica auxilia na redução de riscos associados à escolha de fornecedores não qualificados, que impactam diretamente na etapa de gestão do contrato. Ao exigir que os licitantes demonstrem sua experiência anterior, o órgão licitante pode tomar decisões mais balizadas sobre a capacidade dos fornecedores em entregar o que foi contratado. Sem um atestado de capacidade técnica que comprove a experiência anterior do contratado em projetos semelhantes, pode haver uma maior probabilidade de que a execução do contrato seja de baixa qualidade, uma vez que a falta de experiência pode levar a erros, atrasos, resultados insatisfatórios e até mesmo a inexecução parcial ou total do objeto.
- Concorrência baseada em critérios técnicos: A exigência de atestados de capacidade técnica no Edital promove a concorrência isonômica com base em critérios técnicos, uma vez que todos os licitantes devem atender aos mesmos requisitos mínimos relacionados à integração de soluções de segurança da informação. Isso evita que empresas que apenas fornecem licenciamento de software, que não possuem capacidade operacional, experiência ou aparelhamento técnico, participem da licitação, causando incertezas quanto à entrega do objeto e execução contratual.
- Atendimento aos Princípios da Publicidade e Impessoalidade: A inclusão de requisitos claros, como o atestado de capacidade técnica, demonstra o cumprimento dos princípios de publicidade e impessoalidade, uma vez que as licitantes interessadas e devidamente capacitadas têm acesso às mesmas informações e oportunidades.

2.18.5. Além disso, justifica-se a inclusão do referido item que "Qualificação Técnica" em razão da complexidade e volume do objeto, fazendo-se necessário o licitante demonstrar que já atuou em contratos anteriores com solução de segurança da informação similar e volume de entrega proporcional ao objeto do Edital.

2.18.6. A qualificação técnica deve conter a seguinte redação e atender os seguintes parâmetros:

Considerando as parcelas de maior relevância ou valor significativo do objeto da licitação, os quantitativos e unidade de referência, segue os parâmetros e justificativas dos itens que devem constar na exigência de qualificação técnica.

I - Fornecimento de licenciamento de software, permanente ou por subscrição, solução PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE ON-PREMISE ou AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3), incluindo serviços de parametrização e operacionalização; considerando, a implantação para um mínimo de 7.009 (sete mil e nove) usuários, cujo atestado de capacidade técnica comprove fornecimentos de pelo menos um dos Itens 1, 2 ou 3 (ou similar) desde Termo de Referência.

Justificativa da unidade e quantidade: a unidade de medida adotada é "usuários ativos", conforme indicado nos itens **4.6** e **4.7** do ETP. A quantidade exigida refere-se ao número de usuários para o qual serão aplicadas as licenças de software da Solução de Segurança, cujo valor deve ser comprovado por meio do(s) atestado(s); considerando que o conjunto de licenças adquiridas corresponde à quantidade de usuários do(s) órgão(s). Deste modo, de forma a parametrizar a quantidade exigida, adotamos como referência o valor correspondente à 50% do somatório da quantidade de usuários dos 3(três) maiores Tribunais Regionais Eleitorais, considerando esta a parcela de maior relevância, conforme demonstrado no quadro a seguir.

TRIBUNAL	QUANTIDADE DE USUÁRIOS
TRE-SP	7.019
TRE-MG	4.000
TRE-PR	3000
TOTAL	14.019
50%	7.009

Total: 7.009 usuários.

Obs: Quantidades extraídas do item 13.1 do ETP (Tabela - CONSOLIDAÇÃO LEVANTAMENTO DE INFORMAÇÕES DOS TRIBUNAIS PARTÍCIPES, Ofício-Circular nº 5 / 2023 - TRE-DF/PR/DG/GDG)

O texto anterior também considera a necessidade de comprovação do serviço de implantação de parametrização e operacionalização da solução de Segurança da Informação, serviço acessório ao objeto principal.

II - Prestação de SERVIÇO DE APOIO OPERACIONAL E INVESTIGAÇÃO DE COMPORTAMENTOS SUSPEITOS, ou equivalente, por prazo mínimo de 12 (doze) meses.

Justificativa: O item 6 a que se refere a necessidade de comprovação de qualificação técnica anterior, será contratado por 24(vinte e quatro) meses. Por esse motivo, propomos o ajuste da quantidade para 12(doze) meses, no qual o item de qualificação do respectivo atestado de capacidade técnica corresponda a 50% do especificado para o item 6, correspondente.

III - Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

2.19. Requisitos de Projeto e Implementação

O escopo dos serviços a serem contratados deve abranger a instalação da Solução, implantação, parametrização e operacionalização dos diversos componentes da Solução de Auditoria de Dados e E-mail, além de treinamento e transferência de conhecimento, e apoio operacional para investigação e análise de alertas e comportamentos suspeitos no ambiente do contratante.

Todas as atividades relacionadas à implantação da Solução serão prestadas nas instalações do Contratante pela equipe da Contratada, preferencialmente de forma remota.

Por instalação, customização, integração e ativação entendam-se todos os procedimentos relacionados à instalação e configuração, física e lógica, parametrização e testes de quaisquer componentes de software fornecidos no escopo do Edital, de modo a garantir o pleno funcionamento da solução.

A Contratada deverá criar e manter atualizada documentação das atividades, processos, testes, homologação, entrega e conferência, reuniões de trabalho, compromissos e prazos, incluindo planos de trabalho e atas de reunião, de modo a compor uma documentação final da implantação a ser entregue. Toda a documentação gerada no escopo do projeto deverá estar no idioma Português.

O Contratante se reserva o direito de redefinir, a qualquer momento da implantação, quaisquer fases, ações, prazos e recursos envolvidos, objetivando a garantia de atendimento dos parâmetros de qualidade, segurança, mitigação de riscos e atendimento de prazos, cabendo à Contratada adequar-se às modificações propostas, refazendo atividades e documentação, caso necessário, desde que essas não extrapolem o escopo dos serviços definidos no objeto.

A Contratada será responsável pela execução de quaisquer procedimentos de diagnóstico e solução de problemas relacionados aos serviços de implantação dos componentes da Solução objeto do Edital. Caso o diagnóstico aponte para problemas não relacionados aos componentes da Solução, o Contratante deverá adotar as medidas necessárias para solucioná-los, desde que devidamente comprovados pela Contratada, e sempre a critério do Contratante.

Os serviços de instalação das soluções abrangem as soluções descritas nos itens 1 a 3 da tabela de bens e serviços.

2.20. Requisitos da Arquitetura Tecnológica

A contratação da solução deverá atender aos seguintes requisitos de arquitetura tecnológica.

1. **Servidores:**
    - Suportar a instalação em servidores virtuais dedicados para executar a solução de segurança. A quantidade e a capacidade dos servidores podem variar com base no volume de dados a ser monitorado e na complexidade da implantação.
2. **Sistema Operacional:**
    - A solução deve suportas sistemas operacionais Windows para os servidores onde ele é implantado.
3. **Armazenamento:**
    - Armazenamento suficiente para armazenar os metadados coletados e as informações de auditoria, que podem ser substanciais em organizações com grandes quantidades de dados.
4. **Banco de Dados:**
    - Um banco de dados, como o Microsoft SQL Server, é geralmente necessário para armazenar os metadados coletados e outras informações críticas.
5. **Rede:**
    - A rede deve ser configurada para permitir a comunicação entre os componentes da solução e as fontes de dados a serem monitoradas. O tráfego de rede deve ser configurado para garantir a segurança e a integridade dos dados.
6. **Segurança:**
    - Mecanismos de segurança, como firewalls, antivírus, detecção de intrusão e autenticação de dois fatores, devem ser implementados para proteger o ambiente da solução, quando recomendados pelo fabricante.
7. **Requisitos de Hardware:**
    - Os requisitos de hardware específicos podem variar dependendo das necessidades da implementação.
8. **Software Adicional:**
    - Dependendo da configuração específica, podem ser necessários outros softwares, como servidores de autenticação, servidores de diretório, bancos de dados ou serviços de armazenamento em nuvem.
9. **Conectividade de Dados:**
    - Configuração de conectividade com os sistemas e fontes de dados que serão monitorados pela solução a ser contratada. Isso pode incluir sistemas de arquivos, servidores de email, bancos de dados, entre outros.
10. **Políticas de Segurança e Acesso:**
    - Deve prever a definição de políticas de segurança e acesso para gerenciar como a solução irá monitorar, proteger e auditar os dados.
11. **Backup e Recuperação:**
    - Implementação de estratégias de backup e recuperação para os dados da solução e seu ambiente subjacente.
12. **Requisitos de Desempenho e Dimensionamento:**
    - Planejamento para o dimensionamento e o desempenho da solução de acordo com o crescimento esperado dos dados e das operações da organização.
13. **Licenciamento:**
    - A contratação deve requerer a aquisição das licenças adequadas para as capacidades do ambiente e funcionalidades específicas do software.

3. LEVANTAMENTO DE MERCADO

Fundamentação: Levantamento de mercado, que consiste na análise das alternativas possíveis, e justificativa técnica e econômica da escolha do tipo de solução a contratar (inciso V do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso III da IN 58/2022).

3.1. Avaliação das Diferentes Soluções Disponíveis no Mercado e que Atendam aos Requisitos do Projeto (Levantamento das alternativas)

Preliminarmente, foram levadas em consideração as orientações contidas nos Modelos, Diretrizes e Orientações para Contratação de Soluções de TIC, disponíveis nos seguintes links:

- Diretrizes para a Aquisição de Ativos de Tecnologia da Informação e Comunicação - publicado em 23/03/2017 - Orientações específicas para a aquisição de Ativos de TIC.
- Guia de Boas Práticas em Contratação de Soluções de Tecnologia da Informação do Tribunal de Contas da União.
- Diretrizes para a Aquisição de Ativos de Tecnologia da Informação e Comunicação - Orientações específicas para a aquisição de Ativos de TIC.
- Catálogos de Soluções de TIC com Condições Padronizadas publicados pelo Órgão Central do SISP, onde verificou-se que a solução escolhida não possui item presente, dentre os itens encontrados no referido catálogo (§ 2º do art. 43 da Lei nº 14.133/2021).
- Modelos da Lei 14.133/21 para bens e serviços de TIC da Advocacia-Geral da União.

Deste modo, para elaboração do ETP e TR foram consideradas as orientações para Contratação de bens e serviços de Tecnologia da Informação e Comunicação (TIC), disponíveis no Portal Governo Digital, do **Ministério da Gestão e da Inovação em Serviços Públicos**, disponível em https://www.gov.br/governodigital/pt-br/contratacoes, onde é possível acessar as recomendações e diretrizes para o processo de contratação de soluções de TIC. Naquele portal, também estão disponíveis Guias, Modelos e Diretrizes para Contratações de Solução de TIC de caráter geral e por temas, onde é possível verificar as boas práticas do governo federal na administração e contratação de recursos de TIC. Deste modo, na elaboração do Estudo Preliminar, Termo de Referência e demais documentos de planejamento da contratação para a solução pretendida, foram observados os guias, manuais e modelos publicados pelo Órgão Central do SISP. (IN SGD nº 94/2022, art. 8º, §2)

Também foi consultada a base do Portal de Compras, através do endereço https://www.comprasgovernamentais.gov.br/, que reúne diversos outros pontos de pesquisa, como o sistema Comprasnet, o Painel de Compras (http://paineldecompras.economia.gov.br/) e o Painel de Preços (https://paineldeprecos.planejamento.gov.br/), os quais apresentam dados estruturados de contratações realizadas em todo o país. Essas contratações representam o resultado de uma avaliação das contratações de Soluções de TI pelos Órgãos e Entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação (SISP) do Governo Federal e encontram-se catalogadas e categorizadas por subconjunto de bens e serviços.

Ainda no âmbito da Administração Pública Federal, foi consultado o Portal da Transparência mantido pela Controladoria-Geral da União (http://www.portaltransparencia.gov.br/contratos/), através da pesquisa disponível nas opções “Consulta Detalhada” e após em “Contrato” e também por meio do campo “Busca específica”.

Outra forma de pesquisa se deu por meio da verificação dos contratos dos órgãos pertencentes ao Poder Executivo Federal, por meio de sites de busca, avaliando também como estão se posicionando acerca desse tipo de demanda por solução de TI. Neste caso foram pesquisadas as seguintes palavras chaves: auditoria, microsoft, controle, acessos, diretório, arquivos, active directory, fileserver, servidor de arquivos, ad. Nesse contexto, a partir da definição dos requisitos e dos métodos de pesquisa supracitados, a Equipe de Planejamento da Contratação identificou as seguintes alternativas de mercado:

3.1.1. Pesquisas em contratações públicas

Foi realizada pesquisa para analisar a disponibilidade de solução similar em outro órgão ou entidade da Administração Pública em contratações anteriores, cujo levantamento indicou que os seguintes órgãos realizaram contratações cujo objeto apresentam similaridades às alternativas de solução proposta neste estudo preliminar:

1. AGÊNCIA NACIONAL DE TRANSPORTES TERRESTRES - ANTT (PREGÃO ELETRÔNICO Nº 38/2018)

1.1 Objeto: registro de preços para fornecimento e implantação de solução de auditoria e gerenciamento de serviços (Microsoft Active Directory – AD), servidor de arquivos (Microsoft File Server), correio eletrônico (Microsoft Exchange Server) e solução de análise de comportamento e alarme em tempo real, de uso permanente, incluindo a execução de serviços especializados de apoio pós- implantação, conforme condições, quantidades e especificações contidas no Termo de

1.2 Referência, Anexo I do Edital.

1.3 Itens do pregão:

1.3.1 Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory)

- Produto ofertado: DatAdvantage for Microsoft Active Directory
- Custo: R$ 2.264.400,00, ou R$ 444,00 por usuário, para 5.100 usuários

1.3.2. Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de servidores de Arquivos (Microsoft File Server)

- Produto ofertado: DatAdvantage for Microsoft File Server
- Custo: R$ 2.626.500,00, ou R$ 515,00 por usuário, para 5.100 usuários

1.3.3. Solução de Tecnologia da Informação para auditoria, controle e gerência de permissionamento dos serviços de sistema de correio eletrônico (Microsoft Exchange Server)

- Produto ofertado: DatAdvantage for Microsoft Exchange Server
- Custo: R$ 2.907.000,00, ou R$ 570,00 por usuário, para 5.100 usuários

1.3.4. Solução de Tecnologia da Informação de análise de comportamento e alarme em tempo real

- Produto ofertado: DatAlert
- Custo: R$ 2.907.000,00, ou R$ 570 por usuário, para 5.100 usuários.

1.3.5. 1900 horas de serviços especializados de apoio pós-implantação

- Custo: R$ 456.000,00, ou R$ 240,00 por hora.

1.4. Adjudicado para: OMEGA TECNOLOGIA DA INFORMACAO LTDA

1.5. **Análise**: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

2. MINISTÉRIO PÚBLICO DO TRABALHO/PROCURADORIA GERAL DO TRABALHO - MPT/PGT (PREGÃO MPT/PG/39/2017)

2.1. Objeto: registro de preços para a contratação de empresa especializada no fornecimento de subscrições, com vigência de 12 meses, de software para a auditoria de serviço de diretório Microsoft Active Directory, Servidor de Arquivos Windows Server e portal de autoatendimento para gestão de senhas de usuários, para atender às necessidades do Ministério Público do Trabalho, conforme descrições e quantitativos especificados no Edital e seus anexos;

2.2 Referência, Anexo I do Edital.

2.3. Itens do pregão:

2.3.1. Pacote de subscrição anual de software para auditoria de serviço de diretório Microsoft Active Directory que atenda, no mínimo, 160 controladores de domínio e 7 mil contas de usuário.

- Produto ofertado: Netwrix Auditor for Active Directory
- Custo: R$ 50.024,35

2.3.2. Pacote de subscrição anual de software para auditoria de servidor de arquivos Windows Server que atenda, no mínimo, 160 servidores de arquivos Windows Server e 7 mil contas de usuário.

- Produto ofertado: Netwrix Auditor for File Services
- Custo: R$ 30.019,25

2.3.3. Treinamento para as soluções dos itens 1 e 2.

- Custo: R$ 179,00 por participante

2.3.4. Prestação de serviços especializados para instalação e configuração das soluções ofertadas nos itens 1 e 2, com duração de 20 horas.

- Custo: R$ 4.896,35

2.4. Adjudicado para: AIQON SERVICOS EM INFORMATICA LTDA - ME

2.5. **Análise**: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

3. MINISTÉRIO DA EDUCAÇÃO/INSTITUTO NACIONAL DE ESTUDOS E PESQUISAS EDUCACIONAIS - MEC/INEP (PREGÃO 04/2017)

3.1. Objeto: registro de preços para fornecimento e implantação de solução de auditoria e governança, baseado em software, para ambiente de diretórios de usuários, servidores de arquivos, correio eletrônico Exchange, monitoramento e prevenção de ameaças internas, identificação e classificação de informações sensíveis e automação de permissionamento no âmbito do Inep, contemplando execução de serviços de apoio pós-implantação.

3.2 Referência, Anexo I do Edital.

3.3. Itens do pregão:

3.3.1. Solução de auditoria, controle e gerência de permissionamento dos serviços de AD (Microsoft Active Directory) para 1000 usuários com 36 meses de garantia.

- Produto ofertado: Varonis - DatAdvantage for Directory Services & DatAdvantage Probe SL50
- Custo: R$ 327,00 por usuário.

3.3.2. Solução de auditoria, controle e gerência de permissionamento dos serviços de servidores de Arquivos (Microsoft File Server) para 1000 usuários com 36 meses de garantia.

- Produto ofertado: Varonis - DatAdvantage IDU Analytics (Engine) for Windows
- Custo: R$ 667,00 por usuário.

3.3.3. Solução de auditoria, controle e gerência de permissionamento dos serviços de sistema de correio eletrônico (Microsoft Exchange Server) para 1000 caixas postais com 36 meses de garantia.

- Produto ofertado: Varonis - DatAdvantage for Exchange
- Custo: R$ 660,00 por usuário.

3.3.4. Solução de análise de comportamento e alarme em tempo real de ameaças internas para 1000 usuários com 36 meses de garantia.

- Produto ofertado: Varonis - DatAlert Suite
- Custo: R$ 665,00 por usuário.

3.3.5. Solução de classificação para 1000 usuários com 36 meses de garantia.

- Produto ofertado: Varonis - IDU Classification Framework
- Custo: R$ 663,00 por usuário.

3.3.6. Portal de permissionamento automático para 1000 usuários com 36 meses de garantia.

- Produto ofertado: Varonis - DataPrivilege
- Custo: R$ 668,00 por usuário.

3.3.7. 1.000 horas de serviços de apoio pós-implantação pelo período de 36 meses.

- Custo: R$ 248,00 por hora.

3.4. Adjudicado para: OMEGA TECNOLOGIA DA INFORMACAO LTDA

3.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

4. CONSELHO FEDERAL DE ENGENHARIA ARQUITETURA E AGRONOMIA - CONFEA (PREGÃO 03/2017)

4.1. Objeto: contratação de empresa especializada para fornecimento e instalação de Solução de Auditoria e Gerenciamento de Serviços do AD (Microsoft Active Directory), Servidor de Arquivos (Microsoft File Server), Correio Eletrônico (Microsoft Exchange Server), Solução de Portal de Permissionamento Automático, Solução de Classificação de Dados Sensíveis e Solução de Análise em tempo real e prevenção de comportamentos suspeitos, incluindo, treinamento para operacionalização do software, bem como execução de serviços de planejamento, implementação e testes, além de transferência de conhecimentos e operação assistida, com garantia (manutenção e suporte técnico), de acordo com as especificações e condições gerais constantes neste Edital e seus Anexos.

4.2 Referência, Anexo I do Edital.

4.3. Itens do pregão:

4.3.1. Solução de Auditoria em Microsoft Active Directory

- Produto ofertado: Varonis - DatAdvantage for Directory Services & DatAdvantage Probe SL50
- Custo: R$ 200,00 por usuário.
- Quantidade: 6.375 usuários

4.3.2. Solução de Auditoria em Microsoft Exchange

- Produto ofertado: Varonis - DatAdvantage for Exchange
- Custo: R$ 260,00 por usuário.
- Quantidade: 6.375 usuários

4.3.3. Solução de Auditoria em Windows File Server

- Produto ofertado: Varonis - DatAdvantage IDU Analytics (Engine) for Windows
- Custo: R$ 287,90 por usuário.
- Quantidade: 6.375 usuários

4.3.4. Solução de Portal de Permissionamento Automático Produto ofertado: Varonis - DataPrivilege Custo: R$ 290,00 por usuário.

- Solução de Classificação de Dados Sensíveis
- Produto ofertado: Varonis - IDU Classification Framework
- Custo: R$ 291,67 por usuário.
- Quantidade: 7.125 usuários

4.3.5. Solução de análise em tempo real e prevenção de comportamentos suspeitos

- Produto ofertado: Varonis - DatAlert Suite
- Custo: R$ 293,33 por usuário.
- Quantidade: 7.125 usuários

4.3.6. Serviços de garantia junto ao fabricante software com todas as características detalhadas para Microsoft Active Directory, pelo período de 12 (doze) meses.

- Custo: R$ 50,00 por usuário.
- Quantidade: 7.125 usuários

4.3.7. Serviços de garantia junto ao fabricante software com todas as características detalhadas para Microsoft Exchange Server, pelo período de 12 (doze) meses

- Custo: R$ 65,00 por usuário.
- Quantidade: 7.125 usuários

4.3.8. Serviços de garantia junto ao fabricante software com todas as características detalhadas para Microsoft Windows Server, pelo período de 12 (doze) meses

- Custo: R$ 72,00 por usuário.
- Quantidade: 7.125 usuários

4.3.9. Serviços de garantia junto ao fabricante software com todas as características para Portal de Permissionamento Automático, pelo Período de 12 meses

- Custo: R$ 72,50 por usuário.
- Quantidade: 7.125 usuários

4.3.10. Serviços de garantia junto ao fabricante software com todas as características para Solução de classificação de dados sensíveis, pelo Período de 12 meses

- Custo: R$ 72,50 por usuário.
- Quantidade: 7.125 usuários

4.3.11. Serviços de garantia junto ao fabricante software com todas as características para solução Análise em tempo real e prevenção de comportamentos suspeitos, pelo Período de 12 meses

- Custo: R$ 72,50 por usuário.
- Quantidade: 7.125 usuários Operação Assistida (HORA)
- Custo: R$ 249,50 por hora.
- Quantidade: 3.300 horas

4.3.12. Treinamento Oficial do Fabricante para 3 (três) funcionários

- Custo: R$ 6.000,00 por 3 participantes.
- Quantidade: 15

4.4. Adjudicado para: INFOSEC TECNOLOGIA DA INFORMACAO LTDA

- Custo total: R$ 15.053.175,00

4.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

5. MINISTÉRIO PÚBLICO DO ESTADO DE MATO GROSSO/PROCURADORIA GERAL DE JUSTIÇA - MP/PGT (PREGÃO 077/2016)

5.1. Objeto: contratação de empresa especializada para fornecimento e instalação da Solução de Auditoria e Gerenciamento de Serviços do AD (Microsoft Active Directory), servidor de Arquivos (Microsoft File Server) e Correio Eletrônico (Microsoft Exchange Server), incluindo, transferência de conhecimentos e treinamento para operacionalização do software, bem como execução de serviços de planejamento, implementação e testes, com garantia de atualizações e suporte técnico pelo prazo de 12 meses e demais licenciamentos necessários ao funcionamento da Solução.

5.2 Referência, Anexo I do Edital.

5.3. Itens do pregão:

5.3.1 Licenciamento da solução de auditoria para AD (Microsoft Active Directory) com Serviços de Garantia e suporte do Fabricante

- Produto ofertado: NetAdmin automação e auditoria para Active Directory v4.3
- Custo: R$ 264,96 por usuário.
- Quantidade: 500 usuários

5.3.2. Licenciamento da solução de auditoria para Servidor de Arquivos (Microsoft File Server) com Serviços de Garantia e suporte do Fabricante

- Produto ofertado: NetAdmin auditoria para File Server v4.3
- Custo: R$ 336,00 por usuário.
- Quantidade: 500 usuários

5.3.3. Licenciamento da solução de auditoria para Correio Eletrônico (Microsoft Exchange Server) com Serviços de Garantia e suporte do Fabricante

- Produto ofertado: NetAdmin automação e auditoria para Exchange Server v4.3
- Custo: R$ 336,00 por usuário.
- Quantidade: 1.200 usuários

5.3.4. Banco de Horas de Consultoria para Implementações

- Custo: R$ 2501,00 por hora.
- Quantidade: 200 horas

5.4. Adjudicado para: Egon Tecnologia

- Custo total da contratação: R$ 753.680,00

5.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

6. GOVERNO DO ESTADO DE RONDÔNIA/DEPARTAMENTO ESTADUAL DE TRÂNSITO - DETRAN/RO (PREGÃO 027/2016/DETRAN/RO)

6.1. Objeto: aquisição de licença de software de auditoria, controle e gerência de logs e permissionamento dos serviços de AD (Microsoft Active Directory), Servidor de Arquivos (Microsoft File Server) e Servidor de Atividades de Logon e Logoff, para ambiente Microsoft com instalação e treinamento Hand's-ON, garantia e suporte do fabricante por um período de 36 (trinta e seis) meses de garantia e suporte do fabricante por um período de 36 (trinta e seis) meses, de modo a atender às necessidades do DETRAN/RO, de acordo com a justificativa, quantidades e especificações técnicas mínimas constantes no TERMO DE REFERÊNCIA.

6.2 Referência, Anexo I do Edital.

6.3. Itens do pregão:

6.3.1. Licença de software de auditoria e gerência de logs e permissionamento dos serviços de AD (Microsoft Active Directory)

- Produto ofertado: Dell Change Auditor for Active Directory
- Custo: R$ 190,00 por usuário.
- Quantidade: 1.600 usuários Servidor de arquivos (Microsoft File Server)

6.3.2. Produto ofertado: Dell Change Auditor for Windows File Servers

- Custo: R$ 190,00 por usuário.
- Quantidade: 1.600 usuários Servidor de atividades de logon e logoff

6.3.3. Produto ofertado: Dell Change Auditor for logon activity

- Custo: R$ 214,96 por usuário.
- Quantidade: 1.600 usuários

6.4. Adjudicado para: RL2 Serviço de informática Ltda.

- Custo total da contratação: R$ 594.960,00

6.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

7. TRIBUNAL SUPERIOR ELEITORAL - TSE (PREGÃO 125/2014)

7.1. Objeto: aquisição de Solução de Auditoria em Ambiente Microsoft, com garantia de atualizações e suporte técnico pelo período de 36 (trinta e seis) meses, conforme especificações, condições, quantidades e prazos constantes do Termo de Referência - Anexo I deste edital.

7.2. Referência, Anexo I do Edital.

7.3. Itens do pregão:

7.3.1. Fornecimento do software com todas as características detalhadas para Microsoft Directory (AD), pacote para 500 usuários internos.

- Produto ofertado: Varonis
- Custo: R$ 496.427,00 para 500 usuários.
- Quantidade: 4 pacotes

7.3.2. Fornecimento do software com todas as características detalhadas para Microsoft Windows Server, pacote para 500 usuários internos.

- Produto ofertado: Varonis
- Custo: R$ 929.799,00 para 500 usuários.
- Quantidade: 4 pacotes

7.3.3. Fornecimento do software com todas as características detalhadas para Microsoft Exchange Server, pacote para 500 caixas postais.

- Produto ofertado: Varonis
- Custo: R$ 1.372.680,96 para 500 usuários.
- Quantidade: 4 pacotes

7.3.4. Serviços profissionais de implantação e testes para a solução.

- Custo: R$ 124.567,00
- Quantidade: 1

7.3.5. Serviços profissionais de transferência de conhecimento da solução, por participante.

- Custo: R$ 38.805,00 por participante.
- Quantidade: 7 participantes.

7.3.6. Serviços de suporte técnico para todos os softwares da solução e serviços executados, 8x5, pelo período de 36 (trinta e seis) meses, para a solução.

- Custo: R$ 5.367,00 por mês

7.3.7. Serviços de garantia junto ao fabricante – software com todas as características detalhadas para Microsoft Active Directory (AD), pelo período de 36 (trinta e seis) meses, pacote para 500 usuários internos.

- Custo: R$ 193.308,00para 500 usuários.
- Quantidade: 4 pacotes.

7.3.8. Serviços de garantia junto ao fabricante – software com todas as características detalhadas para Microsoft Windows Server, pelo período de 36 (trinta e seis) meses, pacote para 500 usuários internos.

- Custo: R$ 330.691,00 para 500 usuários.
- Quantidade: 4 pacotes.

7.3.9. Serviços de garantia junto ao fabricante – software com todas as características detalhadas para Microsoft Exchange Server, pelo período de 36 (trinta e seis) meses, pacote para 500 usuários internos.

- Custo: R$ 489.003,00 para 500 usuários.
- Quantidade: 4 pacotes.

7.3.10. Serviços de Apoio pós-implantação pelo período de 36 (trinta e seis) meses, por hora para a solução. Incluem: Operação assistida, integração com novas versões do Windows e do Exchange, integração com sistemas do TSE e estudos de caso.

- Custo: R$ 112.882,00.
- Quantidade: 500.

7.4. Adjudicado para: Vert Solucões em informática Ltda.

- Custo total da contratação: R$ 4.093.529,96

7.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

8. SECRETARIA DE ESTADO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO DO DISTRITO FEDERAL (PREGÃO ELETRÔNICO Nº 001/2023)

8.1. Objeto: Registro de Preços para para a aquisição de solução de detecção e resposta a incidentes, auditoria e proteção de dados, detecção e resposta a ameaças baseadas em dados, coleta fluxos de metadados, e analise constante de dados e de seus repositórios de dados corporativos e dispositivos de perímetro da rede corporativa do GDF, conforme especificações e condições estabelecidas no termo de referência constante do Anexo I do Edital. Vigência 24 meses.

8.2 Referência, Anexo I do Edital.

8.3 Itens do pregão:

8.3.1. Licença de direito de uso, atualização e suporte para solução de análise de comportamentos suspeitos e governança em Windows File Server pelo período de 24 meses.

- Produto ofertado: Varonis Datalert, Varonis Datadvantage for Windows
- Custo: R$ 3.912.000,00
- Quantidade de usuários: 4.000

8.3.2. Licença de direito de uso, atualização e suporte para solução de análise de comportamentos suspeitos e governança em Active Directory e LDAP pelo período de 24 meses.

- Produto ofertado: Varonis Datalert, Varonis Datadvantage for Directory Services Guardian Key GK
- Custo: R$ 2.400.000,00
- Quantidade de usuários: 4.000

8.3.3. Licença de direito de uso, atualização e suporte para solução de análise de comportamentos suspeitos e governança em Correio Eletrônico Exchange Server pelo período de 24 meses.

- Produto ofertado: Varonis Datalert, Varonis Datadvantage for Microsoft Exchange
- Custo: R$ 2.400.000,00
- Quantidade de usuários: 4.000

8.4. Adjudicado para: OMEGA TECNOLOGIA DA INFORMAÇÃO LTDA., inscrita no CNPJ nº 04.808.453/0001-08

- Custo total da contratação: R$ 8.712.000,0000

8.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

9. AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL (PREGÃO ELETRÔNICO Nº 17/2021)

9.1. Objeto: Prestação de SERVIÇOS DE solução de segurança da informação para auditoria, monitoramento e gerenciamento de acessos do ambiente Microsoft da ANEEL, conforme especificações deste Edital e seus anexos.

9.2 Referência, Anexo I do Edital.

9.3 Itens do pregão:

9.3.1. Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Windows File Server

- Produto ofertado: Varonis DatAdvantage para Windows File Server
- Custo: R$ 144.000,00
- Quantidade de usuários: 1.200

9.3.2. Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Microsoft Exchange

- Produto ofertado: Varonis DatAdvantage para Microsoft Exchange
- Custo: R$ 161.844,00
- Quantidade de usuários: 1.200

9.3.3. Renovação da garantia técnica da licença perpétua do módulo Varonis DatAdvantage para Microsoft Active Directory

- Produto ofertado: Varonis DatAdvantage para Microsoft Active Directory
- Custo: R$ 144.000,00
- Quantidade de usuários: 1.200

9.3.4. Subscrição do módulo Varonis

- Produto ofertado: Varonis DatAlert
- Custo: R$ 444.000,00
- Quantidade de usuários: 1.200

9.3.5. DatAlert Subscrição do módulo Varonis Data Classification Framework

- Produto ofertado: Varonis Data Classification Framework
- Custo: R$ 318.048,00
- Quantidade de usuários: 1.200

9.3.5. Serviço de apoio técnico operacional pós-implantação (HORA)

- Custo: R$ 48.102,00
- Quantidade: 300 Horas

9.4. Adjudicado para: OMEGA TECNOLOGIA DA INFORMAÇÃO LTDA., inscrita no CNPJ nº 04.808.453/0001-08

- Custo total da contratação: R$ 1.259.994,00

9.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

10. TRIBUNAL DE CONTAS DO ESTADO DO ALAGOAS

10.1. Objeto: Registro de preços, para futura e eventual fornecimento e implantação de solução de auditoria e governança, baseado em software, para ambiente de diretórios de usuários, servidores de arquivos, monitoramento e prevenção de ameaças internas, identificação e classificação de informações sensíveis e busca de informação não estruturada corporativa, contemplando execução de serviços de apoio pós-implantação.

10.2 Referência, Anexo I do Edital.

10.3 Itens do pregão:

10.3.1. Solução de auditoria e governança, baseado em software, para ambiente de diretórios de usuários, licenciada por 12 meses.

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 568,00
- Quantidade: 50

10.3.2. Solução de auditoria e governança, baseado em software para servidores de arquivos, licenciada por 12 meses.

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 568,00
- Quantidade: 600

10.3.3. Solução de auditoria e governança, baseado em software, para monitoramento e prevenção de ameaças internas, licenciada por 12 meses.

- Produto ofertado: Varonis DatAlert
- Custo: R$ 568,00
- Quantidade: 600

10.3.4. Solução de auditoria e governança, baseado em software, para identificação e classificação de informações sensíveis, licenciada por 12 meses.

- Produto ofertado: Varonis Data Classification
- Custo: R$ 568,00
- Quantidade: 600

10.3.5. Solução de auditoria e governança, baseado em software, para busca informação não estruturada corporativa, licenciada por 12 meses.

- Produto ofertado: Hardware para Solução de auditoria e governança de TI.
- Custo: R$ 399.900,00

- Quantidade: 2

10.4. Adjudicado para: OMEGA TECNOLOGIA DA INFORMAÇÃO LTDA., inscrita no CNPJ nº 04.808.453/0001-08

- Custo total da contratação: R$ 2.191.400,00

10.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo, com exceção do item 6.

11. AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL - ANAC (PREGÃO ELETRÔNICO Nº 28/2019)

11.1. Objeto: Aquisição de licenças perpétuas de software para solução de auditoria, gestão, automação, monitoração e delegação do gerenciamento de serviços do AD (Microsoft Active Directory), correio eletrônico (Microsoft Exchange Server) e servidores de arquivos (Microsoft File Server). A solução deve monitorar os usuários em tempo real, identificar desvios de comportamento, permitir delegação de gerenciamento de acesso aos proprietários dos dados, executar ações proativas em múltiplos objetos, e identificar e classificar conteúdos sensíveis.

11.2 Referência, Anexo I do Edital.

11.3 Itens do pregão:

11.3.1. Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de serviço de diretório (Microsoft Active Directory).

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 1.284.000,00
- Quantidade: 2.400

11.3.2. Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de servidores de arquivos

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 1.066.800,00
- Quantidade: 2.400

11.3.3. Licença perpétua de software de Solução de Tecnologia da Informação para auditoria e outras funcionalidades de correio eletrônico (Microsoft Exchange)

- Produto ofertado: Varonis DatAdvantage para Microsoft Exchange
- Custo: R$ 1.284.000,00
- Quantidade: 2.400

11.3.4. Licença perpétua de software de Solução de Tecnologia da Informação para identificação e classificação de conteúdos sensíveis

- Produto ofertado: Varonis Data Classification
- Custo: R$ 1.066.800,00
- Quantidade: 2.400

11.3.5. Serviços de suporte técnico e garantia

- Custo: R$ 2.664.000,00
- Quantidade: 36 meses

11.3.6. Treinamento para as soluções contratadas

- Custo: R$ 43.000,00 / turma
- Quantidade: 1

11.4. Adjudicado para: INFOSEC TECNOLOGIA DA INFORMACAO LTDA

- Custo total da contratação: R$ 7.285.000,00

11.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

12. TRIBUNAL SUPERIOR DO TRABALHO (CONTRATO PE Nº 58/2021)

12.1. Objeto: aquisição de soluções de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados, endpoint e proteção e controle de acesso de usuários privilegiados (PAM), incluindo garantia, serviço de instalação e treinamento.

12.2 Instrumento contratual

12.3. Itens:

12.3.1. Licença de uso de software e garantia por 12 meses para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados, abrangendo centro de dados e endpoint.

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 5.430.379,50
- Quantidade: 3.129

12.3.2. Licença de uso de software e garantia por 12 meses para funcionalidade de auditoria para disco em nuvem para solução de segurança, auditoria e prevenção de ameaças à base de dados não estruturados.

- Produto ofertado: Varonis DatAdvantage
- Custo: R$ 5.430.379,50
- Quantidade: 3.350

12.4. Adjudicado para: JAMC CONSULTORIA E REPRESENTAÇÃO DE SOFTWARE LTDA

- Custo total da contratação: R$ 7.285.000,00

12.5. Análise: esta contratação está alinhada aos requisitos levantados neste ETP, quanto às necessidades de negócio e tecnológicas descritas no tópico 2.1 deste estudo.

3.1.2. SOLUÇÃO 01 - Contratação de Solução de Mercado

Trata-se da contratação no formato de serviço, com fornecimento de solução de auditoria, proteção de dados, detecção e resposta a ameaças a dados não estruturados e metadados, análise de dados em repositórios corporativos internos (on premises) ou na nuvem em plataformas de colaboração; e serviços agregados de instalação, customização, configuração e treinamento. Verificou-se que é prática comum a aquisição de produtos que compõem a solução de auditoria dos serviços de administração de diretório de usuários (*Microsoft Active Directory*) e servidor de arquivos (*Microsoft File Server*), uma vez que há no mercado uma grande quantidade de revendas autorizadas que atendem a presente demanda, garantindo a sustentação e expansão do uso da tecnologia e capacidade computacional, entre outros fatores.

A Secretaria de Tecnologia da Informação (STI) do TRE-PA tem na estratégia de aquisição de soluções de TI a exigência de bens com garantia técnica de funcionamento fornecido pelo fabricante. No caso da solução pretendida, o prazo de vigência do licenciamento com suporte e garantia sugerida será de 24 (vinte e quatro) meses, proporcionando além da continuidade da solução melhores condições de negociação com os fornecedores em busca de economicidade à Administração.

Além disso, ao incluir os serviços de instalação, implantação, parametrização, operacionalização, treinamento e apoio operacional especializado, garante-se a estabilidade do ambiente, uma vez que os profissionais certificados pela fabricante entregarão a solução funcional, adequada à realidade do ambiente computacional da Justiça Eleitoral, bem como realizarão os ajustes necessários para sua otimização e, por fim, a transferência de conhecimento para os servidores administradores da solução, que terão condições de mantê-la em pleno funcionamento.

Identificação de soluções disponíveis no mercado de TIC

O presente estudo visa à contratação de solução de segurança e proteção de dados, auditoria, gestão, automação, monitoração e delegação do gerenciamento (Microsoft Active Directory) de credenciais e perfis de acesso, serviço de diretório local e em nuvem, correio eletrônico local e em nuvem, contemplando o monitoramento de usuários desvios de comportamento além de permitir delegação de gerenciamento de acesso aos proprietários dos dados, executando ações proativas em múltiplos objetos.

A consecução do objeto tem por finalidade aumentar a resiliência e a capacidade de resposta dos Tribunais Regionais Eleitorais a incidentes cibernéticos, por meio de ferramentas que possuam recursos de classificação avançada de dados e automação, incluindo características de análise de comportamento de usuário (User and entity behavior analytics - UEBA). UEBA é uma solução de segurança cibernética que usa algoritmos e aprendizado de máquina para detectar anomalias no comportamento dos usuários em uma rede corporativa.

Em comparativo para o mercardo apresentado pelo Gartner no documento "*Market Guide for Data-Centric Audit and Protection*", empresas como IBM e Varonis poderiam fornecer ferramentas que atenderiam as funcionalidades acima relacionadas a repositório de arquivos. Quando se analisa a lista de empresas sem considerar a funcionalidade de análise de comportamento, alerta e bloqueio, seria possível adicionar à lista, uma quantidade maior de empresas.

O documento do Gartner está relacionado a ferramentas que forneçam funcionalidades para armazenamento de arquivos em servidores de arquivos, mas não relaciona ferramentas que atendem a necessidades para o ambiente de Active Directory e Exchange. Quando se inclui ferramentas para os três tipos de produtos, a lista fica mais restrita.

Em pesquisas realizadas na internet e considerando também empresas relacionada nos documentos do Gartner, foi possível localizar as ferramentas apresentadas nos quadros a seguir. Elas serão analisadas quanto à capacidade de atender a necessidade da Justiça Eleitoral, suas funcionalidades, a possibilidade de aquisição pelo governo, entre outros critérios. A lista de fabricantes e ferramentas apresentadas abaixo inclui as fabricantes ou parceiros com as quais foi possível realizar contato por haverem respondido a solicitações via e-mail ou através do site do fabricante. Algumas ferramentas já fornecidas para a Administração Pública, conforme apresentado no tópico 3.1.1, não aparecem na lista pois não foi possível contato com o fabricante ou algum parceiro. Por outro lado, estão na lista ferramentas e fabricantes de excelente qualidade que ainda não possuem contrato com a administração.

Deste modo, foi realizado o levantamento inicial de fabricantes/marcas, onde foram identificados seguintes as soluções capazes de atender, em parte ou em sua totalidade, aos requisitos esperados da solução proposta.

FABRICANTE	**MANAGE ENGINE**
Ferramentas	1. AD Audit Plus 2. AD Manager Plus 3. Exchange Reporter Plus 4. Recovery Manager Plus 5. AD 360
Descrição da solução e funcionalidades	A Manage Engine é uma divisão de gerenciamento de TI da corporação Zoho. Ela possui sistemas compreensivos de gerenciamento de TI que fazem o trabalho ficar mais simples e possui mais de 90 produtos e ferramentas. Eles fornecem soluções integradas para otimizar a TI, que incluem gerenciamento de dispositivos ou redes, segurança e sistemas de gerenciamento de usuário. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades do órgão 1. AD Audit Plus: • Permite monitorar e visualizar mudanças no ambiente de servidores Windows, incluindo serviços como • Active Directory, estações de trabalho, servidores de arquivos e servidores do domínio. • Monitora qualquer servidor Windows apresentando relatório de eventos, eventos de sistema ou de tarefas agendadas, ou quaisquer mudanças de políticas e processos. • Active Directory: administradores podem avaliar todos os eventos do domínio, como logon e logoff, auditoria de usuários, grupos, computadores, políticas de grupo (GPO), mudanças em unidades organizacionais (OUs) com a utilização de alertas por e-mail ou dezenas de relatórios predefinidos na ferramenta. • Mantem registros de alterações em diversos objetos do AD, como conteiner, contacts, schema, configuration, site, DNS e permissões. • Servidores de arquivos: avalia de forma segura servidores de arquivos e failover cluster por mudanças em arquivos (criação, modificação ou deleção) e pastas. Permite auditoria de acesso, compartilhamentos e permissões. • Estações de trabalho: monitora todo logon ou logoff de usuário e as ações dos usuários no dia a dia com relatórios detalhados de eventos de logon bem sucedidos ou com falha em estações da rede. • Provê alertas instantâneos na própria aplicação e em alertas por e-mail. • Permite configuração de alertas com base em limites que auxiliam de forma precisa a identificação de problemas.

	2. AD Manager Plus: • É uma ferramenta web que permite gerenciar objetos no AD, caixas postais do Exchange, licenças do Office 365, Skype for Business e outras atividades em série. • Inclui funcionalidades de delegação para a central de atendimento de usuários, workflow, automação, entre outras tarefas de gerenciamento. • Permite provisionar de forma padronizada contas de Exchange ou Lync a partir de modelos pré-definidos. • Permite provisionar contas de usuários novos automaticamente e também arquivar as pastas e revogar permissões quando a conta é bloqueada. • Permite automatizar operações críticas ou rotineiras do AD. • Permite delegação de tarefas de gerenciamento de usuários a gerentes de negócio com a utilização. Permite gerenciar caixas postais compartilhadas, de salas e de equipamentos. • Permite gerar relatórios pré-configurados diversos sobre AD e Exchange. • Permite a delegação de tarefas para os técnicos do serviço de atendimento de usuários dentro de OUs específicas. • Permite delegar tarefas como reconfiguração de senhas, criação de usuários, entre outras. Permite delegar se a elevação de privilégio dos técnicos no AD. • Permite controlar a execução de tarefas automatizadas com o uso de workflow e automatização. Permite automatizar tarefas rotineiras do AD, como limpeza do AD. • Permite configurar fluxos de trabalho com aprovação para a execução de tarefas no AD. 3. Exchange Reporter Plus : • Provê informações de componentes do Exchange, incluindo caixas de e-mail, OWA, listas de distribuição, pasta públicas e seus conteúdos. • Permite identificar caixas inativas ou órfãs e permite a remoção segura delas, além de informações detalhadas sobre cada caixa. • Relatório e análise de tráfego de e-mail entre caixas postais, listas de distribuição e pastas públicas. Permite supervisionar acessos e políticas relacionadas a ActiveSync. • Permite configurar alarmes para detecção de eventos como mudança de permissões, problemas nas bases, logon de usuários não proprietários ou alterações em permissões "send-as". 4. Recovery Manager Plus: • Permite recuperação de objetos do AD, sem necessidade de parar ou reiniciar o serviço. Permite automatização e agendamento de backup de AD. • Permite comparação de mudanças em atributos de objetos ao longo do tempo. Permite restauração singular de objetos ou de seus atributos. 5. AD 360 • É uma solução para gerenciamento de acesso e identidade (IAM) que combina as funcionalidades das soluções de AD da Manage Engine em uma única interface e com single sign-on. • A seguir são apresentados algumas informações adicionais em relação às soluções da Manage Engine: • Não instala agentes nos servidores monitorados e as informações são coletadas com base no log de eventos do Windows. • Em caso de perda de comunicação entre o servidor de auditoria e servidor monitorado, pode ocorrer perda de informação de auditoria, caso o servidor monitorado não mantenha os logs por período superior ao tempo de perda da comunicação. • Não realiza modificações no schema do active directory para integração com AD. • As ferramentas são licenciadas com base na quantidade de domínios a serem monitorados e na quantidade de técnicos que operam as ferramentas • A ferramenta não provê atuação proativa em casos de incidentes de segurança cibernética ou ataques de • malware. • Não provê funcionalidade de alteração de múltiplos objetos em servidores de arquivos, ou automatização de tarefas para servidores de arquivos. • Não provê ferramenta ou funcionalidade para descoberta e classificação de dados. Não provê ferramenta ou funcionalidade de análise comportamental dos usuários.

FABRICANTE	NETWRIX
Ferramentas	1. Netwrix Auditor para Active Directory 2. Netwrix Auditor para servidores de arquivos 3. Netwrix Auditor para Exchange.
Descrição da solução e funcionalidades	A Netwrix Corporation é uma empresa focada exclusivamente em prover uma visão completa para segurança de dados e mitigação de riscos em ambientes híbridos. Com esse foco, eles oferecem em seus produtos funcionalidades mais robustas que ferramentas legadas de auditoria de mudanças. Segundo informações da empresa, centenas de milhares de departamentos de TI ao redor do mundo possuem Netwrix Auditor como solução de auditoria. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Justiça Eleitoral. 1. Netwrix Auditor para Active Directory • A ferramenta provê uma visão completa do que está acontecendo no Active Directory e Group Policy. • Permite detectar todas as alterações do Active Directory e de Group Policy. • Provê detalhes de quem, o que, quando e onde uma alteração foi realizada, e os valores anteriores e posteriores à alteração.

	• Permite auditar logon com relatórios de tentativas de logon ou acesso a sistemas críticos. Fornece histórico completo de logon de qualquer usuário. • Permite comparar o estado atual de usuários, grupos, suas permissões no AD, suas GPOs e suas configurações com um padrão preestabelecido. • Provê relatórios alinhados a controle de padrões internacionais de conformidade do ambiente. • Fornece relatório sobre alterações de configurações de políticas de grupo com detalhamento dos valores anteriores e posteriores à modificação. • Fornece alertas para desvio de padrões de comportamento em alterações do AD, tentativas repetitivas de logon e outras ameaças ao ambiente. • Possui ferramenta de pesquisa refinada sobre os dados auditados. • Fornece descoberta de comportamento anormal de usuários maliciosos e contas comprometidas pela agregação de suas atividades anormais no AD e em outros sistemas críticos. • Simplifica a detecção de possíveis ameaças ao AD, como logons não habituais que poderiam indicar o furto de uma credencial de acesso. • Auxilia na imposição do princípio de contas com baixo privilégio no ambiente. Permite a recuperação de objetos e o retorno à configuração anterior. • Permite identificar usuários inativos, alertas de contas expiradas ou contas bloqueadas. Permite a auditoria de mudanças e logons no AD sem necessidade de agente 2. Netwrix Auditor para servidores de arquivos • Facilita a governança de acesso a dados e um melhor gerenciamento dos dados através de maior visibilidade sobre a atividade em arquivos e do comportamento dos usuários. • Aumenta visibilidade sobre alterações ou acesso suspeito a dados, comportamento anômalo do usuário, direitos de acesso excessivos. • Fornece relatórios que mapeiam as mais comuns regulações de conformidade. • Permite detectar, investigar ou remediar proativamente alterações não necessárias, como deleções acidentais a dados críticos. • Permite a criação de alertas customizados para ameaças, como muitas alterações de arquivos ou tentativas de acesso. • Possui ferramenta de pesquisa refinada sobre os dados auditados. • Provê informação detalhada sobre alterações nos servidores de arquivos para detalhes como quem fez a alteração, o que foi alterado, quando e onde ocorreu a alteração. • Permite a comparação do estado atual e passado de permissões para alinhar com as regras organizacionais de acesso. • Permite a descoberta e classificação de dados sensíveis através da informação sobre que tipo de dados sensíveis a organização possui, onde está localizado, quem possui acesso ao dado e como ele é utilizado. • Alerta para a ocorrência de muitas alterações de arquivos ou tentativas de acesso em um curto período de tempo, o que permitiria responder a ataques ransonware ou atividades de usuários suspeitos. • Provê informação detalhada sobre o proprietário dos dados, o uso dos dados, o volume, os dados duplicados ou obsoletos . • Coleta as informações sem a utilização de agentes e, assim, não interfere no desempenho do sistema e seus processos. 3. Netwrix Auditor para Exchange • Auxilia na detecção e investigação de comportamento de usuários suspeitos. • Permite visualização de eventos críticos de acesso e mudanças, permitindo detecção de atividades suspeitas e rápida resposta. • Provê relatórios predefinidos de conformidade com padrões internacionais. • Ajuda a minimizar problemas de e-mails ao permitir aos administradores detectar problemas e identificar a causa raiz. • Permite identificar acesso de usuário não proprietário a caixa de e-mail, incluindo informações sobre quem acessou qual e-mail, quando e de onde foi acessado o e-mail. Além disso, permite identificar o conteúdo que foi lido, alterado, copiado ou deletado. • Possui ferramenta de pesquisa refinada para identificar a causa raiz e para ajudar a identificar como um evento de alteração ou acesso ocorreu. • Permite responder rapidamente a atividades suspeitas e prevenir proativamente o vazamento de dados com alertas customizados para determinados padrões de ameaça. • Notifica atividades suspeitas que podem comprometer a segurança de informações sensíveis ou a disponibilidade do serviço de e-mail. A seguir são apresentadas algumas informações adicionais em relação às soluções desta empresa: • Não instala agentes nos servidores monitorados e as informações são coletadas com base no log de eventos do windows. • Em caso de perda de comunicação entre o servidor de auditoria e servidor monitorado, pode ocorrer perda de informação de auditoria, caso o servidor monitorado não mantenha os logs por período superior ao tempo de perda da comunicação • Não realiza modificações no schema do active directory para integração com AD. • As ferramentas são licenciadas com base na quantidade de contas ativas de colaboradores no AD e de contas de serviço ou sistema ativas no AD. • As ferramentas desta empresa são focadas exclusivamente em auditoria e, assim, não fornecem funcionalidade para administração do AD, servidores de arquivos ou Exchange. Também não fornecem funcionalidades para ações proativas em casos de incidentes de segurança cibernética e ataques de malwares. • As ferramentas possuem funcionalidade para descoberta e classificação de dados. As ferramentas possuem funcionalidade de análise comportamental dos usuários.

FABRICANTE	VARONIS
Ferramentas	1. Varonis DatAdvantage para Directory Services

	2. Varonis DatAdvantage para Windows 3. Varonis DatAdvantage para Exchange 4. Varonis DataPrivilege 5. Varonis IDU Classification Framework 6. Varonis DataAlert 7. Varonis Data Governance Suite
Descrição da solução e funcionalidades	A Varonis é uma empresa pioneira em segurança e análise de dados, especializada em segurança, governança, conformidade, classificação e análise de dados. Suas ferramentas permitem detectar ameaças internas e ataques cibernéticos pela análise da atividade sobre arquivos e análise do comportamento do usuário. Também é possível a prevenção de desastres, o bloqueio de dados sensíveis e a sustentação de um estado seguro dos dados com automação. As soluções da empresa aproveitam metadados para que as organizações possam, de maneira inteligente, acessar, governar, migrar e dispor de seus dados não-estruturados. Baseadas em uma tecnologia patenteada e em ferramentas de análise precisa, as soluções fornecem às organizações total visibilidade e controle dos seus dados, garantindo que somente os usuários corretos tenham acesso aos dados corretos. Todo o uso é monitorado, e o abuso, assinalado. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades do órgão. 1. Varonis DatAdvantage para Directory Services • É construído para apresentar, filtrar e analisar estruturas hierárquicas grandes e complexas, estendendo as capacidades das ferramentas de administração padrão. • Permite auditar quem fez alterações no Active Directory, e quando elas foram realizadas. • Fornece uma trilha de auditoria que inclui alterações em grupos, OUs e políticas de grupo (GPO) para qualquer período de tempo. • Permite auditar as alterações de configuração, as mudanças recentes em políticas de senhas, quem realizou e de qual computador foram realizadas a mudança nas políticas de grupo (GPOs) do AD. Fornece recomendações para grupos não utilizados e associações a grupos. • Permite identificar associações de grupo excessivas para uma remoção segura e sem afetar o processo de negócio. • Permite modelar alterações sem afetar o ambiente de produção. • Permite visualizar a hierarquia de serviços de diretórios pela ferramenta DatAdvantage GUI. • Permite visualizar domínios, OUs, computadores, grupos e outros objetos de domínio pela ferramenta DatAdvantage GUI. • Permite gerar alertas em tempo real para eventos de interesse, com a ferramenta Varonis DatAlert Ferramenta pode ser estendida com a funcionalidade de classificação de dados com a ferramenta IDU Classification Framework. • Usuários de negócio e proprietários de dados podem ser envolvidos diretamente com a ferramenta DataPrivilege. 2. Varonis DatAdvantage para Windows • É uma solução que agrega informações de eventos sobre usuários, permissões, dados e acessos a diretórios e servidores de arquivos. • A informação coletada é analisada para fornecer informações detalhadas de uso e determinar o acesso correto baseado em um necessidade de negócio. • Permite visibilidade completa sobre a estrutura de permissões dos servidores Windows. • Mostra os dados acessíveis a cada usuário ou grupo, assim como usuários e grupos com permissões a uma pasta. • Identifica pastas que necessitam de um proprietário. • Fornece uma trilha de auditoria de cada arquivo dos servidores monitorados. Permite pesquisa rápida sobre os dados normalizados, processados e armazenados. • Realiza a coleta de informações de auditoria com o mínimo impacto para os servidores de arquivos e sem a necessidade de habilitar a auditoria nativa do Windows. • Permite identificar permissões não necessárias em grupos e em arquivos para uma remoção segura e sem afetar o processo de negócio. • Realiza alterações em objetos do AD e ACLs em uma interface única. • Identifica os proprietários de negócio dos dados pela análise estatística da atividade dos usuários. Gera relatórios automatizados e personalizados para envolver proprietários dos dados no processo de governança de dados. • Ferramenta pode ser estendida com a funcionalidade de classificação de dados com a ferramenta IDU Classification Framework. • Permite gerar alertas em tempo real para eventos de interesse com a ferramenta Varonis DatAlert. • Permite identificar mudanças em membros de grupos e em permissões. • Permite modelar e simular mudanças em permissões sem afetar o ambiente de produção. 3. Varonis DatAdvantage para Exchange • É uma solução que agrega informações de eventos sobre usuários, permissões, dados e acessos a caixas de e-mail e pastas públicas do Exchange. • A informação coletada é analisada para fornecer informações detalhadas de uso e determinar o acesso correto baseado em um necessidade de negócio. • Permite visibilidade completa sobre as permissões no Exchange. Fornece uma trilha de auditoria para toda atividade de e-mail. • Permite detectar picos de uso repentino na atividade de e-mail. • Fornece recomendações para remoção de excesso de permissões e modelagem de mudanças. Identifica os proprietários do dados de negócio pela análise estatística da atividade dos usuários. Mostra os dados acessíveis a cada usuário ou grupo no ambiente de e-mail, assim como toda caixa postal ou pasta pública que pode ser acessada por um usuário ou grupo. • Identifica e ajuda a corrigir excesso de permissões de acesso aos recursos. • Monitora qualquer evento de e-mail e mudança de permissões no ambiente do Exchange. Permite pesquisa rápida sobre os dados normalizados, processados e armazenados.

- Realiza a coleta de informações de auditoria com o mínimo impacto para os servidores monitorados. Realiza a análise da atividade no ambiente de e-mail em busca de atividades anormais,
- como worms, vírus e spam.
- Permite remover com segurança associações de grupo excessivas sem afetar o processo de negócio, através da combinação de informação sobre quem pode acessar um dado e a trilha de auditoria de quem o está acessando.
- Permite modelar e simular mudanças em permissões sem afetar o ambiente de produção. Identifica os proprietários de negócio dos dados pela análise estatística da atividade dos usuários.
- Relatórios sobre o acesso aos dados, a atividade, as mudanças em pastas e grupos, e os dados obsoletos podem ser providos automaticamente aos proprietários dos dados.

4. Varonis DataPrivilege

- É uma ferramenta que permite dar aos usuários do negócio o poder de revisar e gerenciar o controle de acesso a pastas, arquivos ou grupos de segurança sem a assistência da TI e sem necessidade de direitos administrativos.
- Permite garantir que o acesso a grupos, listas de distribuição e dados sensíveis de negócio seja revisado constantemente pelas pessoas certas.
- Algoritmos de aprendizado marcam os usuários que não deveriam mais ter acesso, facilitando a revisão dos acessos.
- Fluxos de autorização permitem aos usuários requisitar acesso por uma interface web. Cada requisição é direcionada ao proprietário correto baseado em fluxos pré-definidos.
- A resposta a requisições de acesso pode ser dada com a resposta a um e-mail.
- Após a aprovação de uma requisição de acesso, o acesso é garantido pela ferramenta DataPrivilege sem o envolvimento da TI.
- Permite atribuir data de validade a uma autorização e garantir que seja revogada automaticamente. Permite automatizar acesso ou revogar acesso baseado em atributos dos usuários.
- Permite auditar todas as alterações.
- Autorizações, revisões de direitos e outros relatórios gerenciais fornecem evidências da aderência ao processo e ajudam a atender a requisitos de conformidade.
- O processo de revisão de acesso, geração de relatórios e modificações é feito diretamente via navegador web.
- Permite configurar agendamentos para revisões de direitos de acesso com base em departamento, em informações sensíveis, ou outros tipos de informação.

5. Varonis IDU Classification Framework

- Permite visualizar onde os dados mais sensíveis para a organização estão armazenados. Permite recomendar como o acesso ao dado sensível pode ser reduzido.
- Permite classificar dados sensíveis com base em expressões regulares, padrões pré-definidos de conteúdo ou busca por conteúdo baseada em dicionário, incluindo auto atualização de dicionários. Permite busca incremental para os novos dados criados ou modificados e não necessita de uma busca completa a cada nova verificação.
- Permite criar regras de classificação baseadas em conteúdo e em metadados.
- Permite criar buscas por palavras chave em arquivos, metadados de arquivos, frases ou expressões regulares.
- Fornece resultados de classificação precisos por usar algoritmos de verificação, como IBAM, Luhn e Verhoeff.
- Permite coletar metadados sobre usuários e grupos, permissões de quem pode acessar um dado e a atividade de quem está acessando o dado, para fornecer informações eficientes sobre a atividades realizadas sobre a informações.
- Permite obter alertas em tempo real para eventos de interesse, como arquivos sensíveis que foram deletados ou modificados com a ferramenta Varonis DatAlert.
- Permite incorporar a informação de classificação de conteúdo produzida pelo motor de classificação de conteúdo da Varonis ou por um fonte externa de classificação de metadados, como RSA DLP.

6. Varonis DataAlert

- É um sistema que permite detectar e alertar sobre atividades suspeitas em sistemas de arquivos e e-mail.
- Permite monitorar ativos críticos em busca de atividades suspeitas ou comportamento anormal de usuários.
- Permite monitorar eventos em plataformas Windows, Unix/Linux, NAS, AD, Sharepoint ou Exchange. Permite detectar falhas potenciais de segurança, falhas de configuração ou outros problemas.
- Permite a redução do tempo total necessário para detectar e corrigir problemas nos ativos.
- Permite detectar ameaças com a utilização de modelos preditivos de ameaças com base em análise avançada, comportamento do usuário e aprendizado automático de maquina.
- Permite a defesa contra ameaças internas, códigos maliciosos como ransonware, e violações de dados. Possui um painel web que permite pontuar, triar, analisar, priorizar alertas e tomar ações para resolução de incidentes.
- Permite implementar ações personalizadas com a execução de linhas de comando. Pode ser integrado com SIEM e soluções de gerenciamento de redes.
- Por detrás dos modelos de ameaças baseadas no comportamento dos usuários, há uma equipe de especialistas em segurança e cientistas de dados trabalhando continuamente.

7. Varonis Data Governance Suite

- É uma solução para governança de dados que se utiliza de uma estrutura de dados extensível e escalável para prover inteligência organizacional sobre seus dados.
- É uma solução que está integra as outras soluções como DatAdvantage, DataPrivilege e IDU Classification Framework.
- Permite automatizar o processo de revisão e autorização de acessos.
- Permite a aplicação de políticas nos dados de infraestrutura e garantir conformidade regulatória. Permite a aplicação automática de aprovações e revogações de acessos aos arquivos.
- Fornece uma trilha de auditoria para todo evento de acesso.
- Permite a identificação de acessos excedentes para removê-los e fornece a possibilidade de simular alterações sem afetar o ambiente de produção.

	• Permite classificar dados sensíveis ou críticos ao negócio de forma precisa e rápida.

FABRICANTE	STEALTHBITS
Ferramentas	1. StealthAUDIT for Active Directory 2. StealthAUDIT for File Systems 3. StealthAUDIT for Exchange 4. StealthBits Sensitive Data Discovery and Classification 5. StealthAUDIT Action Modules 6. StealthINTERCEPT
Descrição da solução e funcionalidades	A STEALTHbits Technologies Inc. é uma companhia de sistemas de segurança cibernética focada na proteção dos dados sensíveis e na proteção contra credenciais roubadas para ataque aos dados das organizações. A empresa permite às organizações reduzir o risco de segurança, atender a requisitos de conformidade e diminuir os custos de suas operações pela remoção de acessos inapropriados, pela aplicação de políticas de segurança e pela detecção de ameaças avançadas. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades do órgão. 1. StealthAUDIT for Active Directory • É um modelo estruturado para auditoria, conformidade legal e normativa, e governança que provê coleta de dados, análise, recuperação e relatórios para combater os desafios de complexidade, segurança e gerenciamento enfrentados pelas organizações. • Não utiliza agentes para execução de suas funções. Por isso, possui coleta rápida e com pouca carga sobre os sistemas. • Possui dezenas de relatórios pré-configurados e permite a criação de relatórios personalizados rapidamente. • Permite a configuração de fluxos de trabalho alinhados a segurança, conformidade legal e gerenciamento operacional. • Coleta informações de objetos e seus atributos, políticas de grupo (GPOs), configurações, membros de grupos, domínios, sites, relações de confiança, ou qualquer informação do AD. • Permite identificar e configurar proprietários de grupos. Permite automatizar a revisão de associações a grupos. • Permite descentralizar (self-service) o gerenciamento de grupos e requisições de associações a grupos. Realiza coleta, inventário e análises sobre permissões a todos os objetos e permite compreender quem possui acesso privilegiado no Active Directory (AD). • Verificações pré-configuradas e personalizáveis de boas práticas de segurança permitem identificar proativamente configurações críticas de segurança que deixam o AD vulneráreis a ataques. • Permite identificar objetos obsoletos, duplicados ou problemáticos e limpá-los de forma automatizada. Permite automatizar a produção de artefatos de conformidade pelo fornecimento de relatórios pré-configurados e personalizáveis alinhados a vários padrões de conformidade, como HIPAA, PCI-DSS, GDPR e SOX. 2. StealthAUDIT for File Systems • É uma ferramenta que permite à organização satisfazer requisitos de conformidade legal e reduzir seu risco de exposição através do controle completo e automatizado de governança de acesso a dados não estruturados residentes em servidores de arquivos. • Permite reduzir o risco de ameaças internas, perda de dados sensíveis e condições não desejadas de acesso livre em servidores de arquivos. • Provê um fluxo automatizado para identificação de proprietários dos dados. Permite confirmar a correta propriedade de um dado. • Reúne detalhes completos de permissões de acesso a compartilhamentos, pastas e arquivos e permite identificar condições anormais como quebra de herança, SIDs com problema, permissões diretas de usuários e acesso amplo permitido. • Correlaciona informação do AD com informação coletada nos compartilhamentos para determinar como um usuário pode acessar um recurso e também o nível de permissão do usuário. • Coleta metadados de arquivos para compreender tudo o que é necessário sobre um arquivo, incluindo tipo, atributos, proprietários e outros rótulos. • Permite identificar o proprietário mais provável de um compartilhamento ou pasta, incluindo gerentes comuns, criadores de conteúdos e usuários mais ativos. • Monitora atividade em sistemas de arquivos NAS e Windows para uma visão completa de quais arquivos, pastas ou compartilhamentos os usuários estão acessando, assim como o que eles fazem com os dados. • Permite identificar onde os dados sensíveis estão armazenados para entender onde o risco de acesso existe e poder fortalecer as iniciativas de prevenção de perda de dados. • Permite rotular automaticamente arquivos com suas classificações necessárias. Fornece suporte a sistemas de arquivos locais ou em nuvem. • Permite coletar apenas informações necessárias à auditoria através de um escopo granular e flexível, e de um controle dos eventos monitorados. • Identifica e movimenta automaticamente dados obsoletos ou dados sensíveis em casos de necessidade de redução de custos de armazenamento e diminuição de riscos aos dados. 3. StealthAUDIT for Exchange • É uma ferramenta que provê uma visão profunda do Exchange local ou Online, pela combinação da coleta, análise e readequação dos dados. • Fornece uma visão ampla sobre como o acesso está ou foi provisionado no Exchange. • Provê uma visão global sobre caixas de e-mail, pastas públicas, membros de listas de distribuição e PSTs, que inclui detalhes específicos do tipo de acesso garantido a cada usuário. • Permite aos administradores obter métricas de uso do sistema de e-mail, com a compreensão de quem usa o que, a frequência de utilização, ou se os recursos são ainda necessários.

	• Permite diminuir os riscos de segurança e os eventos de vazamentos de informações. • Permite reduzir o número de recursos não necessários ou obsoletos. • Permite reduzir os custos do atendimento de serviços pela resolução de pequenos problemas proativamente. • Permite otimizar o desempenho pela diminuição do impacto de usuários poderosos na infraestrutura crítica. • Permite auditar o acesso de um não proprietário a uma caixa de e-mail. 4. StealthBits Sensitive Data Discovery and Classification • Fornece às organizações a habilidade de procurar por mais de 400 tipos de conteúdos, que incluem imagens, informação sensível, números sociais e dezenas de outros tipos de informações sociais. Permite a criação de critérios únicos a cada organização, como número de identificação de empregados, chaves de segurança, formulas de produtos ou outros tipos. • Permite coletar metadados de arquivos, incluindo rótulos aplicados por processo internos da organização ou outra ferramenta, assim como aplicar rótulos que identificam o nível de sensibilidade do arquivo, conteúdo ou outra designação. • Permite gerar relatórios pré-configurados ou personalizados que podem ser rotulados para fácil identificação. • Permite a revisão dos dados encontrados no ambiente pelos responsáveis, a marcação de falsos positivos e a inspeção de arquivos com informação sensível. 5. StealthAUDIT Action Modules • Permite aos usuários readequar diversas condições identificadas durante o processo de coleta e análise em série de dados, assim como organizar fluxos de trabalho para automatizar processos manuais ou procedimentos associados ao AD, servidores de arquivos, Sharepoint, Exchange ou outras ferramentas. Os módulos de ação são habilitados dentro do StealthAUDIT e existem para os serviços de AD, sistemas de arquivos, caixas postais do Exchange, entre outros. • O módulo de ação para AD fornece operações como histórico de limpeza e configuração de SID; mudanças de detalhes ou atributos de objetos de computadores; criação de usuários; remoção de objetos de usuário, grupos ou computadores; desativação ou habilitação de usuários; modificação de membros de grupos; movimentação de objetos; configuração ou reconfiguração de senhas de usuários; ou desbloqueio de usuários. • O módulo de ação para AD permite, por exemplo, automatizar processos de negócio como desativação de contas de rede após a saída de um colaborador, limpeza de objetos obsoletos ou não necessários, ou sincronização de atributos de objetos com sistemas de HR. • O módulo de ação para sistemas de arquivos fornece operações como alterações de atributos; alterações de permissões e auditoria; alteração em permissões de herança; alteração em permissões de compartilhamento; cópia de arquivos; execução de processos remotos; movimentação de arquivos; remoção de permissões; remoção de permissões compartilhadas; e alterações de nomes. • O módulo de ação para sistemas de arquivos permite automatizar funções do ciclo de vida dos dados, permitindo localizar arquivos obsoletos ou não utilizados, movimentá-los para tipos de armazenamento menos custosos ou remover os dados em série, de acordo com a necessidade que se deseja implementar. Esse módulo também poderia ser utilizado para a marcação de arquivos ou a gravação de atributos que permitiriam iniciativas para prevenção da perda de dados, business intelligence (BI) ou classificação dos dados. • O módulo de ação para caixas de e-mail fornece operações como remoção de conteúdos em caixas de correio; alterações em permissões; remoção de permissões; delegação de caixas de e-mail; remoção de delegações; e remoção de SIDs obsoletos. • O módulo de ação para caixas de e-mail permitiria, por exemplo, remediar acessos privilegiados a caixas de e-mail, com a remoção de permissões de contas administrativas que não deveriam mais ter permissão e com a diminuição da exposição inapropriada de dados. 6. StealthINTERCEPT • É uma solução de monitoramento em tempo real de acesso e alterações realizada no AD, sistemas de arquivos e Exchange. • É capaz de identificar ataques a sistemas de arquivos ou ataques baseados em autenticação, monitorar o uso e o abuso de contas privilegiadas, e detectar alterações críticas realizadas no ambiente. • É capaz de iniciar um controle preventivo que bloqueia os ativos críticos e força políticas de escrita. Previne mudanças e atividades que põe em risco a organização • Protege objetos críticos de alterações ou acessos não autorizadas e previne abuso de credenciais. Automatiza a geração de artefatos de conformidade críticos alinhados a padrões regulatórios da indústria. • Correlaciona dados de ameaça fornecendo informações sobre técnicas de ataque e comportamento, sem a necessidade dos logs nativos do sistema operacional. • Monitora mudanças, acessos ou consultas a objetos críticos, e tentativas de comprometimento de credenciais. • Detalhes compreensíveis para cada evento melhoram a visibilidades e tornam os dados mais utilizáveis. Alerta qualquer destino sobre eventos críticos em tempo real em níveis globais ou de acordo com políticas específicas. • Permite execução de ações avançadas usando automação simples e funcionalidades de scripts.

FABRICANTE	**SAILPOINT**
Ferramentas	1. SecurityIQ for Active Directory 2. SecurityIQ for Windows and Unix File Shares 3. SecurityIQ for Exchange

Descrição da solução e funcionalidades	A Sailpoint é uma empresa fundada em 2005 que provê soluções inovadoras para problemas de negócio e um ambiente de trabalho colaborativo relacionado a identidades. Segue uma descrição das principais funcionalidades das ferramentas providas pela empresa que estariam associadas às necessidades da Justiça Eleital. 1. SecurityIQ for Active Directory • É uma ferramenta que permite proteger efetivamente o AD e que provê uma visão completa sobre usuários, grupos, recursos e qualquer atividade associada a eles. • Permite prover uma prova de conformidade durante auditorias e reduzir o tempo gasto em análises forenses. • Permite monitorar e responder a atividades em tempo real • Permite ampliar a estratégia de gerenciamento de identidades de acesso (IAM - Identity Access Management) e prover uma governança de acessos ampla a dados não estruturados. • Permite identificar e limpar contas obsoletas, automatizar requisitos de auditoria e agilizar revisões e requisições de acessos, que permitem reduzir a carga de trabalho da área de tecnologia. • Provê monitoramento de atividades baseado em um contexto de segurança, que permite identificar e responder a violações rapidamente. • Permite monitorar ações como criação, remoção, recuperação, movimentação, alteração de atributos, e adição e remoção de permissões a objetos. • Permite auditar alterações de políticas. • Permite monitorar alterações na regra FSMO (Flexible Single-Master Operation) do AD. Permite monitorar alterações nas políticas de domínio. • Permite monitorar bloqueio de contas, reconfigurações de senha e logons de conta de rede. Permite monitorar ações como modificação de situação; modificação de filtros de segurança; • modificação de propriedades; modificação, adição, modificação ou remoção de links; e histórico de alterações sobre objetos de política de grupos (GPO). • Permite a execução de ações em tempo real com base nas atividades monitoradas para o tratamento de comportamentos arriscados. • Permite o envio de alertas em tempo real por e-mail, assim como execução de ações remotas como verificação ou modificação de acessos. • Permite enviar ou receber alertas para a tomada de ações de governança como notificações, suspensões de contas ou outras. • Realiza coleta e análise automática de todos os direitos em ambientes do Active Directory • Permite identificar quem possui acesso a qual dado. • Permite identificar violações de gerenciamento de acesso ou práticas ruins de gerenciamento. Auxiliar na correção de problemas de governança como combinações não recomendadas de grupos de permissões ou remoção de grupos cíclicos. • Permite aos proprietários dos dados ter visibilidade sobre os dados que possuem, configurar alertas, fornecer acesso controlado por meio de solicitações de acesso com autoatendimento, ou adicionar e remover acessos de alto risco de forma automática. 2. SecurityIQ for File Shares • É uma ferramenta que permite estender controles de governança de identidades a dados sensíveis armazenados em arquivos. • Permite descobrir dados sensíveis expostos espalhados entre uma diversidade de compartilhamentos de arquivos. • Permite identificar, classificar e dar segurança a dados sensíveis armazenados em repositórios locais ou na nuvem, de acordo com regulações como GDPR e HIPAA. • Permite coletar e analisar automaticamente permissões de acesso ou modificação em arquivos. A partir disso, é possível corrigir problemas de acesso para melhorar a segurança dos dados. • Ajuda a identificar e escolher proprietários para os dados. • Painéis práticos alertam os proprietários dos dados sobre riscos de exposição a serem corrigidos, e permitem gerenciar as requisições e revisões de acesso aos dados. • Além de permitir responder quem possui acesso a qual dado, permite revelar dados expostos e outras violações ou práticas ruins de gerenciamento de acesso. 3. SecurityIQ for Exchange • É uma ferramenta que permite ter uma compreensão completa das atividades e modelos de permissão do Microsoft Exchange, além de não afetar a performance do ambiente protegido. • Determina quem tem acesso ao dado, como o dado é utilizado e aplica controles em tempo real para dar segurança ao dado. • Provê uma prova de conformidade durante auditorias e reduz o tempo gasto em análises forenses. Amplia a estratégia de governança de identidades de acesso provendo governança de acesso aos dados não estruturados. • Identifica dados e contas obsoletas. Automatiza requisitos de auditoria. Agiliza a revisão de acessos. • Reduz a carga de trabalho da área de TI. • Fornece monitoramento ativo baseado em contexto com alertas em tempo real. • Toda atividade monitorada é enriquecida com um contexto completo de segurança de sistemas de segurança como Ad. O contexto completo é importante para identificar violações e responder rapidamente, além de auxiliar em análises forenses. • Coleta e analisa todos os direitos concedidos a colaboradores ou em pastas públicas, incluindo permissões "Send As" e "Send on Behalf". • Permite identificar dados expostos. • Permite a escolha dos proprietários dos dados e provê um conjunto de painéis que fornecem inteligência sobre os dados que os proprietários possuem. • A ferramenta cobre tanto Exchange local quanto Exchange Online dentro da mesma licença, suportando assim arquiteturas híbridas do Exchange. • Simplifica solicitações de acesso e gerencia revisões periódicas e revisões baseadas em acesso. • Automatiza o provisionamento e a revogação de acessos.

Os fabricantes e as ferramentas apresentadas nos quadros acima mostram que existem diversos tipos de ferramentas disponíveis no mercado e que cada uma das ferramentas é capaz de oferecer funcionalidades distintas. Um desafio desse estudo é conseguir identificar as ferramentas que estão efetivamente alinhadas à necessidade da Justiça Eleitoral. Por isso, a seguir será apresentado um quadro comparativo que avalia as funcionalidades levantadas a partir das necessidades de negócio/tecnológica para cada uma das ferramentas elencadas nos quadros acima.

COMPARÇÃO DAS SOLUÇÕES DE MERCADO COM BASE NOS PRINCIPAIS REQUISITOS

		FABRICANTES				
		Manage Engine	**Netwrix**	**Varonis**	**StealthBITS**	**SailPoint**
FUNCIONALIDADES	**Active Directory**					
	Auditoria de contas, computadores e grupos	Sim	Sim	Sim	Sim	Sim
	Auditoria de sites, GPO e outros recursos	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	-	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	Sim	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Automatiza tarefas repetitivas, comuns ou complexas	Sim	-	Sim	Sim	Sim
	Delegação de gerenciamento sobre grupos de segurança aos proprietários	-	-	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	Sim	Sim	Sim	-
	Servidores de Arquivos					
	Auditoria de acesso, modificação e remoção de arquivos e pastas	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	-	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	-	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Automatiza tarefas repetitivas, comuns ou complexas	-	-	Sim	Sim	Sim
	Delegação de controle de acesso a proprietários	-	-	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	Sim	Sim	Sim	-
	Microsoft Exchange					
	Auditoria de acesso, modificação e remoção de caixas postais e listas.	Sim	Sim	Sim	Sim	Sim
	Execução de ações proativas com base na auditoria	Sim	-	Sim	Sim	Sim
	Execução ações em múltiplos objetos	-	-	Sim	Sim	Sim
	Gera alertas com base nas informações auditadas	Sim	Sim	Sim	Sim	Sim
	Monitoramento e análise de comportamento de usuários	-	Sim	Sim	Sim	-
	Descoberta e classificação de arquivos em repositórios não estruturados					
	Identificação e classificação de conteúdos sensíveis	-	Sim	Sim	Sim	Sim
	Permitir descoberta e classificação de dados sensíveis e trilha de auditoria de acesso dos usuários aos dados armazenados em nuvem corporativa Microsoft, Google ou AWS.	Sim	Sim	Sim	Sim	Sim
	% de atendimento dos requisitos	**50%**	**54%**	**100%**	**100%**	**86%**

ANÁLISE GERAL DAS SOLUÇÕES DE MERCADO E CONTRATAÇÕES

Pela tabela anterior, é possível constatar que as ferramentas fornecidas pelas fabricantes Varonis e StealthBITS, dentre as que foram avaliadas neste estudo, possuem atentem as necessidades levantadas no tópico 1.2, que detalham os requisitos tecnológicos da solução.

É possível identificar que a ferramenta da SailPoint atende quase todas as funcionalidades definidas, com exceção da funcionalidade de análise e monitoramento de comportamento dos usuários.

É possível identificar uma gama de ferramentas intermediárias, representadas pelos fabricantes Manage Engine e Netwrix. Essas ferramentas entregam funcionalidades de auditoria, porém se diferem quanto à possibilidade de execução de ações, envio de alertas e identificação e classificação de conteúdos sensíveis.

Conforme verificado na lista anterior, considerando a dificuldade em obter as funcionalidades desejadas a partir do desenvolvimento interno da solução, muitos órgãos tem optado pela contratação diretamente no mercado.

Tomando por base as contratações apresentadas, é possível identificar as soluções das empresas Varonis, Dell, NetAdmin e Netwrix em diversas contratações públicas. Não foram identificadas nas contratações as soluções Manage Engine, StealthBITS e SailPoint.

As soluções mencionadas - o ADAudit Plus, SISA Radar, SolarWinds (ARM) e Varonis DatAdvantage, são soluções de segurança cibernética projetadas para ajudar as empresas a proteger seus dados. Cada uma dessas soluções tem suas próprias vantagens e recursos exclusivos, e compará-las pode ajudar a entender melhor suas diferenças e semelhanças.

O ADAudit Plus é uma solução de gerenciamento de logs que permite que as empresas monitorem a atividade de logon e logoff, a atividade de Active Directory, o acesso a arquivos e pastas, entre outros. O ADAudit Plus possui uma interface intuitiva e oferece recursos de conformidade, permitindo que as

empresas atendam a requisitos de regulamentação, como HIPAA, PCI DSS e GDPR. No entanto, o ADAudit Plus não fornece recursos avançados de análise comportamental avançada para detecção de atividades suspeitas e comportamentos anômalos, fornecidos por outras soluções como Varonis DatAdvantage.

O Varonis DataAdvantage é conhecido por sua capacidade de monitorar e auditar o acesso aos dados em tempo real. Ele fornece visibilidade granular sobre quem tem acesso aos dados, como eles estão sendo usados e quais atividades estão sendo realizadas. Além disso, o Varonis DataAdvantage oferece recursos avançados de detecção de ameaças, identificando comportamentos anômalos e indicadores de comprometimento para ajudar a prevenir violações de dados.

O Netwrix Auditor para Active Directory Plus é uma solução focada na auditoria e monitoramento de mudanças no Active Directory, oferecendo auditoria detalhada, geração de relatórios personalizados e alertas em tempo real, enquanto o Varonis DatAdvantage concentra-se na segurança de dados e proteção de arquivos, fornecendo análise de dados, monitoramento de acesso a arquivos e automação de privilégios, com ambos oferecendo facilidade de uso e integração com outras soluções de suas respectivas empresas, tornando a escolha entre eles dependente das necessidades específicas de auditoria de diretrizes ativas ou proteção de dados e controle de acesso a arquivos

O StealthBITS é conhecido por sua especialização em auditoria e controle de acesso a dados não estruturados, oferecendo recursos avançados de monitoramento e auditoria para proteger informações confidenciais, enquanto o Varonis DatAdvantage é uma solução abrangente de segurança de dados que se concentra na análise de dados e permissões, bem como no monitoramento de atividades de acesso a arquivos e recursos de dados, com destaque para a detecção de ameaças internas. A escolha entre essas soluções dependerá das necessidades específicas da organização em relação à proteção de dados não estruturados e à governança de acesso, com ambas oferecendo recursos de geração de relatórios e integração com outros produtos para uma abordagem completa de segurança de dados.

Em comparação com as soluções mencionadas, o Varonis DatAdvantage se destaca por sua análise comportamental avançada, recursos de gerenciamento de acesso granulares e suporte para várias plataformas de armazenamento de dados. O DatAdvantage é altamente personalizável e pode ser adaptado às necessidades específicas de uma organização, fornecendo recursos de auditoria e conformidade avançados, permitindo atender requisitos regulatórios, como LGPD.

Além disso, convém ressaltar que o software Varonis incorpora recursos avançados de inteligência artificial (IA) para aprimorar as funcionalidades de análise e proteção de dados. Esses recursos de IA permitem identificar padrões, comportamentos e anomalias nos dados e comportamento dos usuários de Rede, fornecendo informações e trilhas de auditoria para identificação de ameaças, atendendo os requisitos e características da contratação em tela.

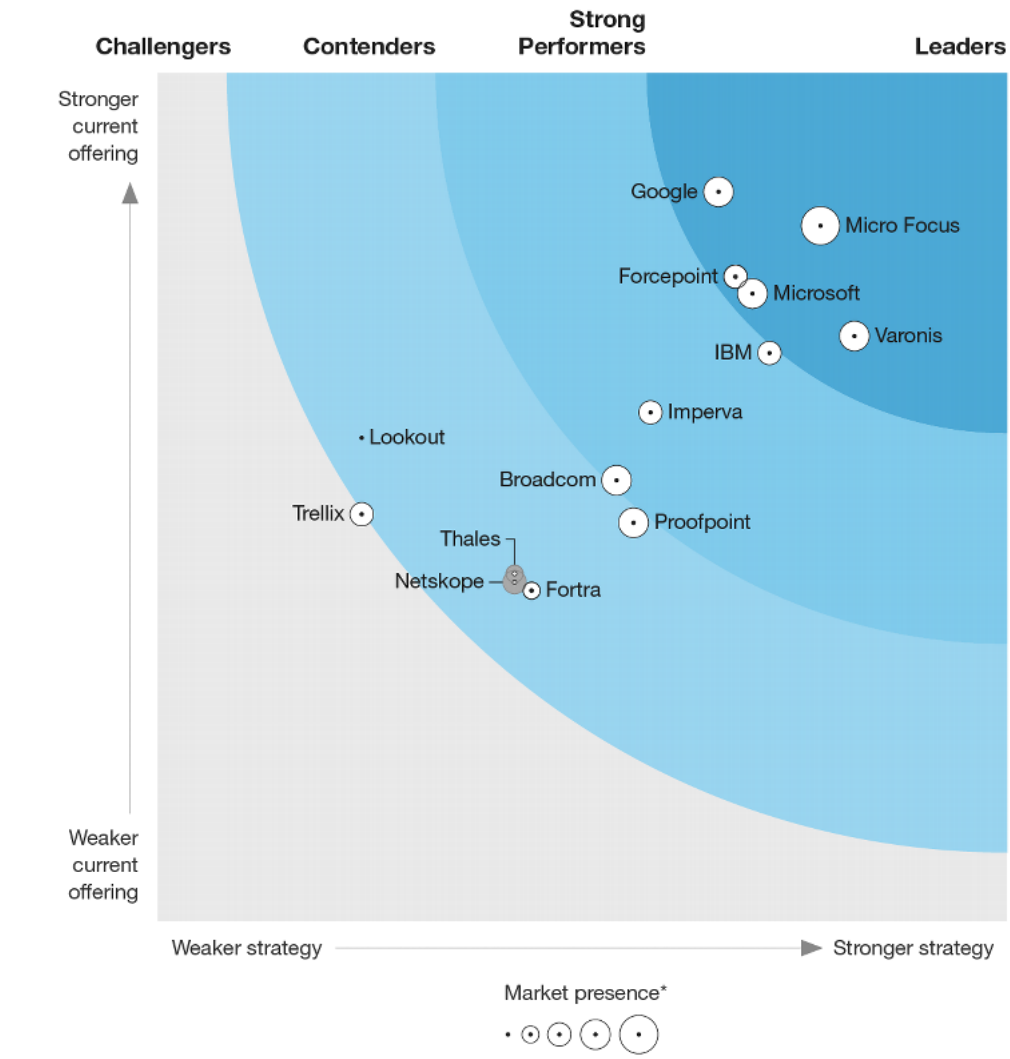
ANÁLISE DO FORRESTER WAVE

Uma vez que torna-se inviável avaliar o posicionamento de todas as soluções e opções disponíveis, recorreu-se a fonte de pesquisa reconhecido no mercado de Tecnologia, a Forrester Wave. O Forrester Wave, é referência na área de consultoria em soluções de Tecnologia da Informação e foi utilizada para delimitar as melhores opções a serem consideradas na análise de soluções disponíveis para as soluções da categoria *Data Security Platforms*. O Forrester Wave possui um “quadrante”, onde são utilizados diversos critérios para avaliar a qualidade e o posicionamento de mercado das soluções.

Como esta Justiça Especializada preza isonomia e qualidade técnica das soluções para compor sua infraestrutura de segurança, as soluções consideradas na análise foram as que se enquadram nos quadrantes “Leaders” e “Strong Performers” do quadrante mais recente, publicado pela The Forrester Wave™ no primeiro trimestre de 2023. Os fabricantes localizados neste quadrante foram avaliados com os melhores resultados em suas soluções oferecidas para plataforma de segurança de dados.

FIGURE 1

Forrester Wave™: Data Security Platforms, Q1 2023



*A gray bubble or open dot indicates a nonparticipating vendor.

Source: Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Ao que podemos verificar no quadrante do Forrester Wave, existem fabricantes líderes em soluções de *Data Security Platforms*, como, por exemplo: Micro Focus, Force Point, Varonis, Microsoft.

3.1.3. SOLUÇÃO 02 - Uso de Software Livre/Público e/ou Open Source

Além das soluções de mercado, existem também baseadas soluções em Software Livres e Open Source. No entanto, a Equipe de Planejamento da Contratação não encontrou soluções que pudessem atender os requisitos elaborados para a contratação em tela.

Visando abordar outros aspectos técnicas e funcionais relacionados à interoperabilidade, assim como quanto à possibilidade de atender a demanda via Software Livre/Público, foram considerados ainda as seguintes consultas.

- Soluções existentes no portal de Software Público Brasileiro (http://www.softwarepublico.gov.br)
  - Não foram identificadas soluções no Portal do Software Público Brasileiro capazes de atender plenamente as necessidades e requisitos desta contratação. Portanto, as alternativas baseadas em software livre ou open source propostas são bastante limitadas, ou inexistentes, dependendo dos requisitos, se comparadas com os recursos disponíveis em softwares comerciais.
- Observância às políticas, premissas e especificações técnicas definidas no Modelo Nacional de Interoperabilidade (MNI) do Poder Judiciário.
  - Não se aplica por tratar de uma solução que não possui o requisito para intercâmbio de informações de processos judiciais e assemelhados entre os diversos órgãos de administração de justiça, nem tampouco servir de base para implementação das funcionalidades pertinentes no âmbito do sistema processual, nos termos tratados pela Resolução Conjunta CNJ/CNMP nº 3 de 16/04/2013.
- Aderência às regulamentações da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil), quando houver necessidade de utilização de certificação digital, observada a legislação sobre o assunto.

    - As alternativas de solução levantadas são capazes de fazer uso dos recursos tecnológicos disponíveis em certificados digitais, estando alinhadas à Infraestrutura de Chaves Públicas – ICP Brasil e em conformidade com a MP nº 2.200-2 – de 24 de agosto de 2001 - e demais arcabouços normativos aplicáveis a solução, instituídos pelo Instituto Nacional de Tecnologia da Informação (ITI).
- Observância às orientações, premissas e especificações técnicas e funcionais definidas no Modelo de Requisitos para Sistemas Informatizados de Gestão de Processos e Documentos do Poder Judiciário (Moreq-Jus)
    - Não se aplica por tratar de uma solução que não possui o requisito de gestão de processos e documentos, nos termos tratados pela Resolução CNJ nº 91 de 29/09/2009.

Ainda, conforme demonstrado neste ETP, a solução pretendida requer a contratação de serviços agregados, como treinamentos, suporte especializado para implantação e operação. Deste modo, mesmo que houvesse solução em software livre que pudesse atender alguns requisitos almejados, as tarefas para integração, implantação e manutenção da solução sobre a equipe de Segurança demandariam elevado tempo até que seja alcançado um nível de maturidade e proteção minimamente adequado. Além disso, entendemos ser inevitável a necessidade de integração de diferentes softwares e soluções, na maioria das vezes, sem a possibilidade de suporte especializado externo.

Outrossim, no contexto de softwares livres, ocorre demanda esforços técnicos de integração, desenvolvimento e customização de partes solução, como scripts e configuração customizada. Neste cenário, por contar com um quantitativo de equipe reduzida para a administração da segurança da informação, os tribunais não poderiam contar com o auxílio de contratação de empresas especializadas para solucionar problemas técnicos que poderiam surgir.

Cumpre registrar que o quadro de servidores da Justiça Eleitoral que atuam especificamente na área de segurança cibernética, como ocorre em outros órgãos da APF, é reduzido e que com o advento de novos projetos da Estratégia Nacional de Cibersegurança, assim com a crescente a demanda de serviços, gerada por esses novos sistemas sobrecarregou, sobremaneira, os trabalhos afetos às Secretarias de TIC, sem contudo, aumentar o quadro funcional que já vinha defasado de mão de obra especializada.

Neste cenário, a solução poderia tornar-se limitada ou insuficiente para resolução de ataques emergentes e, um eventual incidente, a correlação e análise detalhada das informações contidas nos softwares de diferentes fontes poderia levar horas ou dias, comprometendo a investigação dos eventos, a preservação de evidências e a disponibilidade e segurança da rede.

Dessa forma, uma vez que a Instituição não conta com profissionais especializados em quantidades necessárias para a operacionalização das atividades de desenvolvimento e customização dos softwares livres, esta alternativa foi descartada.

3.2. Justificativa de escolha da Solução de TI em relação ao alinhamento às necessidades de negócio e macrorrequisitos tecnológicos, bem como aos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade

Por todo exposto, a Equipe de Planejamento da Contratação recomenda a **SOLUÇÃO 01 - Contratação de Solução de Mercado, por meio da *"Contratação no formato de serviço, com fornecimento de solução de auditoria, proteção de dados, detecção e resposta a ameaças a dados não estruturados e metadados, análise de dados em repositórios corporativos internos (on premises) ou na nuvem em plataformas de colaboração; e serviços agregados"***. O detalhamento dos itens que irão compor a solução de TI, bem como o detalhamento dos valores estimados foram discriminados no item 6.1. ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA.

A eficácia da contratação se justifica no fato de que os bens e serviços a serem contratados são importantes para assegurar o gerenciamento do diretório de usuários e servidor arquivos, permitindo sua auditoria de modo mais assertivo, garantindo a continuidade da produtividade dos servidores e magistrados, e, consequentemente, a prestação jurisdicional à sociedade.

A Equipe de Planejamento da Contratação entende que a vantagem da contratação está na padronização e alinhamento às práticas de mercado, por possibilitar o uso de soluções modernas, padronizadas e amplamente utilizados por vários Órgãos e empresas públicas/privadas, conforme demonstrado no item **3.1.1. Pesquisas em contratações públicas**. Acrescente ainda a total compatibilidade com o ambiente computacional, da facilidade de instalação e operação, não demandando qualquer "arranjo tecnológico" para o pleno funcionamento, eliminando o risco de paralisação ou comprometimento do ambiente computacional da Justiça Eleitoral.

A escolha da solução considerou a melhor adequação entre as necessidades institucionais, o atendimento aos requisitos indispensáveis e a análise das comparações e vantagens das soluções de mercado descritas no item 3.1.2.

Os subitens a seguir elencam as justificativas para a escolha da solução e os benefícios diretos e indiretos pretendidos com a contratação. O objeto da contratação deve possuir as seguintes características:

- Contratação de empresa especializada para prestação de serviços de solução de segurança da informação, com fornecimento de solução de auditoria, proteção de dados, detecção e resposta a ameaças a dados não estruturados e metadados.
- A solução deve prover análise de dados em repositórios corporativos internos (on premises) ou na nuvem em plataformas de colaboração.
- A contratação deve prever os seguintes itens de licenciamento:
    - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES.
        - Justificativa: Auditoria, análise comportamental e proteção de dados para o ambiente Windows Microsoft Active Directory e File Server ou Linux e NAS
    - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES.
        - Justificativa: Auditoria, análise comportamental e proteção de dados para a solução de E-mail Microsoft Exchange *on premise* ou *online.*
    - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES
        - Justificativa: Auditoria, análise comportamental e proteção de dados para ambiente de nuvem (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3).
- A contratação deve incluir serviços de instalação, configuração e operacionalização, além de suporte técnico e serviço de apoio operacional pelo período de 24 meses, e treinamento para as equipes do TRIBUNAL REGIONAL ELEITORAL DO PARÁ e TRIBUNAIS partícipes.

3.2.1. Dos benefícios diretos

A contratação pretende alcançar os benefícios diretos listados a seguir em termos de:

a) Eficácia

- Garantir o acesso efetivo e seguro dos usuários do TRE-PA aos recursos computacionais suportados pelo ambiente MS Windows com a redução dos riscos de ataques cibernéticos; e
- Atender às demandas específicas da Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD) - Resolução CNJ nº 396/2021

b) Eficiência

- Atualizar e ampliar os recursos tecnológicos de segurança da infraestrutura por intermédio de processos de auditoria mais eficientes;
- Aumentar a disponibilidade dos sistemas corporativos finalísticos e operacionais baseados na plataforma MS Windows do TRE-PA;
- Melhorar a capacidade de gestão das auditorias técnicas;

c) Economicidade

- Manter solução de custo agregado compatível com o ciclo de vida dos sistemas de auditoria técnica; e
- Adequar o custo benefício relativo à atualização dos sistemas em uso.

3.2.2. Dos benefícios indiretos

Os benefícios indiretos decorrentes da contratação podem ser considerados em razão das consequências do alcance de todos os benefícios diretos anteriormente listados e refletem valores positivos objetivos, estando a seguir listados:

- Manutenção da imagem do TRE-PA , bem como da Justiça Eleitoral, pela garantia da qualidade de acessibilidade aos serviços; e
- Redução de esforços e melhoria da dinâmica dos processos de auditoria com a atualização tecnológica pretendida.
- Aprimoramento da segurança do processo eleitoral.

3.2.3. Do período da contratação

A contratação do software de Auditoria de Dados não Estruturados (AD, e-mail, compartilhamento de arquivos interno ou na nuvem), por um período de 24 (vinte e quatro) meses pode ser justificada com base nos seguintes argumentos:

- Implementação eficiente: A implementação de um software com a complexidade mencionada neste projeto requer tempo para implantação, o que envolve instalar, configurar, integrar com sistemas existentes, treinar usuários e estabelecer as melhores práticas de uso. Ao contratar por um período de 24 meses, é possível obter um tempo razoável para implementar a solução de forma adequada e garantir que ela esteja totalmente operacional e otimizada para atender às necessidades do Tribunal.
- Retorno sobre o investimento (ROI): O software em questão é uma solução abrangente que oferece recursos de governança de dados, proteção de dados, monitoramento de atividades, detecção de ameaças e mitigação de riscos. Ao contratar por um período de 24 meses, o órgão terá tempo suficiente para explorar todas as funcionalidades do software, obter insights valiosos sobre seus dados e obter um ROI significativo em relação ao investimento realizado.
- Consolidação e padronização: Contratar a solução por um período mais longo permite que a organização consolide e padronize seus processos de segurança e governança de dados. Durante os 24 meses, será possível implantar a solução de forma eficiente no ambiente do Tribunal, garantindo uma abordagem uniforme em toda a organização. Isso resultará em uma maior eficiência operacional, redução de riscos e melhor conformidade com as regulamentações de proteção de dados.
- Acompanhamento e evolução: A contratação do Varonis por um período mais longo proporciona à organização a oportunidade de acompanhar as mudanças no ambiente de segurança cibernética e adaptar a solução de acordo. Durante os 24 meses, podem surgir novas ameaças, regulamentações ou requisitos de segurança, e a organização poderá utilizar a expertise do Varonis para se manter atualizada e garantir uma postura de segurança robusta.
- Monitoramento por maior período: A contratação do software por um período de 24 meses também oferece a vantagem de garantir a continuidade da solução e um monitoramento constante para mitigar ataques cibernéticos. O software, objeto da contratação, possui recursos avançados de detecção de ameaças e monitoramento de atividades, permitindo identificar comportamentos suspeitos, acessos não autorizados e outras atividades maliciosas. Com um monitoramento de forma continuada, por período maior, a organização pode identificar prontamente possíveis ataques cibernéticos e tomar medidas imediatas para mitigar os riscos, garantindo ainda economia de escala, evitando diversas contratações recursivas em razão da manutenção continuada da segurança do Tribunal.

O prazo de vigência do contrato resultante do processo licitatório será de 24 (VINTE E QUATRO) meses contados da assinatura do contrato, prorrogável na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

3.3. Condições de aquisição e pagamento semelhantes às do setor privado (Art. 40, I, da Lei 14.133/21)

No processo de aquisição dos referidos bens, conduzimos uma análise minuciosa das condições de mercado, bem como das práticas utilizadas pelo setor privado em relação a esse tipo de contratação. Nossa equipe realizou pesquisas de mercado, consultou fornecedores especializados e analisou as práticas comumente adotadas pelo setor privado ao adquirir bens similares.

Com base nessas análises, garantimos que o processo de aquisição e pagamento dos bens em questão seguirá condições semelhantes às do setor privado. Isso implica em buscar a melhor relação custo-benefício, levando em consideração a qualidade dos produtos, a eficiência na entrega, a adequação às necessidades da nossa instituição e a competitividade do mercado.

Além disso, adotaremos critérios claros e transparentes na seleção dos fornecedores, buscando aqueles que apresentem as melhores propostas, levando em conta não apenas o preço, mas também a qualidade dos produtos e serviços oferecidos.

Ressaltamos que nosso objetivo é garantir uma contratação justa, eficiente e economicamente viável para a nossa instituição, seguindo as melhores práticas do setor privado.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO (descrição/especificação do Objeto)

Fundamentação: descrição da solução como um todo, inclusive das exigências relacionadas à manutenção e à assistência técnica, quando for o caso (inciso VII do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso IV da IN 58/2022).

Trata-se de demanda de contratação de solução de auditoria e controle em ambiente Microsoft, contemplando serviço de instalação, treinamento, configuração, garantia, atualização e suporte técnico, tendo como finalidade atender as necessidades do Tribunais da Justiça Eleitoral.

A solução de segurança deve permitir que os tribunais rastreiem, visualizem, analisem e protejam seus dados não estruturados. A solução deve executar funcões de *User Behavior Analytics* para identificar comportamentos anormais e defender os dados do órgão contra ataques cibernéticos. O software deve usar metadados coletados da infraestrutura da organização para mapear relacionamentos entre usuários, objetos de dados, conteúdo e uso fora do padrão reconhecido.

A solução deve mapear permissões e quem acessa dados nos sistemas de arquivos on premise e em nuvem. Ele deve mostrar onde os usuários têm acesso que violam o princípio de privilégio mínimo, permitindo automatizar as alterações com segurança para acessar listas de controle e grupos de segurança.

4.1. Das características gerais da solução

I. CONSIDERAÇÕES GERAIS

1. Visando preservar harmonia entre todos os elementos da solução, a total interoperabilidade de componentes e a facilidade de uso e operação, a solução de auditoria deverá ser de um único fabricante;

2. A solução deve disponibilizar console web ou cliente que poderá ser acessada através do servidor de aplicação e estações de trabalho dos usuários com acesso autorizado;

3. A solução deverá possibilitar integração, de forma direta ou indireta, de suas informações com sistemas de DLP (Data Lost Prevention) e SIEM.

4. Caso seja necessária instalação de qualquer agente nos servidores a serem monitorados, o processo não deve impactar na disponibilidade dos servidores ou serviços;

5. O agente deve possuir um mecanismo de monitoramento de desempenho dos servidores onde atua, de modo a não permitir que o nível de consumo de recursos ultrapasse limites definidos e configuráveis;

6. A solução deve oferecer a possibilidade de configurações de diferentes níveis de segurança às suas funcionalidades, podendo, desta forma, ser utilizada por diferentes equipes com variadas demandas de atividades e com acesso restrito a diferentes funções;

7. Devido às características e criticidade das informações coletadas, armazenadas e processadas, com o intuito de garantir integridade e confiabilidade jurídica, contratual e regulatória, e pela possibilidade das informações serem utilizadas para perícia forense inclusive como provas judiciais, a solução deverá ter certificação utilizada pela administração pública como parâmetro para definição de requisitos de sistema de gerenciamento de segurança da informação como a ISO/IEC 27001 ou similares;

8. A solução deve suportar a utilização de servidores virtualizados para os componentes;

9. A solução deve possibilitar a configuração de credencial diferente para cada servidor/serviço a ser monitorado;

10. A solução deverá fazer recomendações de melhores práticas a serem aplicadas no ambiente.

II. RELATÓRIOS

1. A solução ofertada deve gerar relatórios em diversos formatos de arquivos;

2. A ferramenta deve permitir que relatórios sejam extraídos sob demanda uma única vez ou agendados e enviados com frequência definida;

3. A ferramenta deve permitir o agendamento para envio de relatórios pelo correio eletrônico ou para um compartilhamento no servidor de arquivos;

4. A ferramenta deve fornecer relatório de todas as permissões de determinado usuário nos repositórios monitorados.

5. A ferramenta deve fornecer relatório de todos os usuários com permissões em determinada pasta.

6. A ferramenta deve fornecer relatório dos acessos aos arquivos;

7. Fornecer relatórios de dados e usuários inativos;

8. A solução deve fornecer relatório de histórico de permissões;

9. A solução deve fornecer relatório de histórico de membros de grupos de segurança;

10. A solução deve oferecer relatórios de estatísticas, métricas e gráficos com informações sobre usuários, grupos, pastas e permissões ao longo de determinado período;

11. Fornecer relatório dos alertas de comportamento anômalo identificados;

12. A solução deve fornecer relatório com as recomendações de revogação de permissão gerados pela análise comportamental realizada sobre os usuários e recursos monitorados;

13. A solução deve oferecer relatório de estatística de acesso, utilização por tipo de arquivos, eventos por usuários e distribuição por tipos de eventos;

14. A solução deve fornecer relatório de auditoria das ações dos usuários na console;

15. A solução deve oferecer relatório sobre as alterações, versão alterada e quais foram as mudanças realizadas em GPOs.

III. REGISTRO DE EVENTOS (LOG)

1. A solução deve coletar o log das plataformas monitoradas de forma contínua e automática e normatizar essas informações em banco de dados as informações das plataformas monitoradas;

2. A solução deve apresentar todos os logs de todos os usuários na mesma console de visibilidade de permissionamento da plataforma monitorada;

3. Os logs apresentados pela solução ofertada devem conter informações completas de cada uma das operações com data e horário, nome do servidor, tipo do objeto, caminho (path) dos dados, domínio, arquivo impactado e nome do usuário;

4. A solução deverá permitir filtragem gráfica, ordenação e agrupamento dos logs;

5. A solução deverá permitir que os usuários realizem pesquisas baseadas em critérios como: data do evento, servidor ou plataforma em que o evento ocorreu, tipo de evento, arquivos ou diretórios acessados;

6. Deve ser possível alterar o conjunto de dados (colunas) retornados da consulta aos logs de acordo com a necessidade da informação.

4.2. Dos aspectos técnicos da solução

- Permitir um gerenciamento completo sobre os dados e arquivos, quanto a classificação, propriedade, origem, consumo, restrições e volume (tamanho e quantidade);
- Permitir a análise e classificação de riscos dos dados e arquivos;
- Análise e classificação dos dados, destacando dados confidenciais, sensíveis, sigilosos e restritos;
- Análise preventiva na manipulação e comportamento de arquivos e dados, buscando detectar, indicar e alertar quanto a anomalias, duplicações e possíveis ameaças;
- Alerta de acesso/uso indevido de dados e arquivos classificados como confidenciais, sensíveis, sigilosos e restritos;
- Analisar, proteger, monitorar e gerenciar a integridade das informações armazenadas e disponibilizadas no ambiente do TRE-PA melhorando mecanismos de:
  - Controle de acesso;
  - Monitoramento de acesso de usuários normais e privilegiados;
  - Estrutura e perfis do Active Directory (AD);
  - Estrutura das permissões de compartilhamento de arquivos;
  - Conformidade de uso dos sistemas com as regulamentações e requisitos de auditoria aplicáveis do TRE-PA.
- Encontrar arquivos com dados sensíveis, on-premises e/ou na nuvem nos seguintes Ambientes: Windows Server, Sharepoint, OneDrive, Office365, etc;
- Aplicar rótulos e medidas de segurança automaticamente por meio de classificação dos arquivos armazenados em repositórios não estruturados, mapeando onde os dados estão expostos;
- Automação de controle de privilégios: monitorar, alterar e remover, de forma automatizada, privilégios e/ou permissões em arquivos e diretórios que estejam de maneira desnecessária.
- Gerar metadados importantes para investigação forense, resposta a ataques e vazamentos de informações, bem como a análise comportamental dos usuários da rede computacional reduzindo ataques internos, perda de informações e má gestão dos repositórios dos dados não estruturados:
  - Quem acessou? Quando? A partir de que máquina? Quais pastas e arquivos foram acessados? Esses arquivos possuem informações sensíveis? (Classificação dos dados armazenados em repositórios não estruturados, mapeando onde e para quem os dados estão expostos.)
  - Identificação de acessos indevidos de usuários internos mal-intencionados;
  - Dados de LGPD acessados ou compartilhados;
  - E-mails acessados, enviados, marcados como lidos ou não lidos;
  - Pastas criadas abertas, apagadas e renomeadas;
  - Acessos negados;
  - Arquivos compartilhados com pessoas externas através do Sharepoint Online, OneDrive e outros.
  - Quem criou ou habilitou uma conta de usuário, quem definiu uma nova senha e adicionou ou removeu o usuário do grupo de segurança? Quando foi feita e que acessos o usuário ganhou?
- Permitir uma melhora nas respostas ao tratamento de incidentes de segurança da informação através do fornecimento de funcionalidades que permitam a rastrear os eventos, bem como a auditoria dos mesmos, diminuindo os riscos de perda de dados e informações.
- Permitir ações proativas em casos de incidentes de segurança cibernética.

- Realizar a análise comportamental de usuários, a detecção e identificação de ameaças e comportamentos anômalos, gerar alertas de eventos suspeitos em tempo real, permitindo automatização eficiente da execução de ações proativas e configuráveis para casos definidos como críticos conforme as recomendações da equipe CTIR/GSI Presidência da República, quanto ao acesso a dados e recursos armazenados no ambiente monitorado.
- Aumentar o nível de atendimento e qualidade das operações de serviços de TI.
- Aprimorar a governança de Dados e de TI.

4.3. Do suporte:

- A ferramenta deverá suportar ambientes de rede com servidores Windows e Linux;
- A ferramenta deverá suportar a análise a dados e estruturados e não estruturados;
- O fornecedor deverá dar todo o suporte necessário a instalação e configuração da ferramenta no ambiente de rede do TRE-PA;

4.4. Do uso da solução:

- Treinamento aos usuários da ferramenta quanto ao seu uso e funcionalidades;

4.5. Da governança e controle da solução:

- A solução deverá apresentar interface gráfica de fácil uso;
- A solução deverá apresentar as informações em forma de relatórios e gráficos para controle de seu uso bem como dos dados e arquivos.

4.6. Do quantitativo de licenças da solução para cada item

- Para o objeto em questão, o quantitativo de licenças necessário para a contratação leva em consideração o levantamento de usuários ativos cadastrados no Serviço de Diretório (MS Active Directory), Serviços de Correio Eletrônico (MS Exchange) e/ou ambiente de nuvem.
- Quanto aos usuários ativos deve-se considerar tanto os cadastros de usuários de TI: magistradas(os), servidoras(es), colaboradoras(es), estagiárias(os); assim como os usuários de sistemas. A atividade e comportamento desses usuários deverá ser objeto de monitoramento da solução.

4.7. Justificativa do quantitativo de bens e serviços a ser contratado

4.7.1. A Equipe de Planejamento da Contratação apresenta abaixo a forma de estimativa para o quantitativo de bens a serem contratados, cujo detalhamento foi embasado na quantidade atualmente instalada nas Unidades contempladas.

4.7.2. Destaca-se que a contratação de solução em tela inclui o fornecimento de licenças de uso de software, garantia e manutenção, serviços de instalação/configuração, treinamento e suporte técnico especializado, nos termos deste Estudo Preliminar.

ITEM	DESCRIÇÃO	NATUREZA	QUANTIDADE	JUSTIFICATIVAS / NECESSIDADES
1	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇA DE SOFTWARE, BENS INTANGÍVEIS	38.396	• Justificativa da contratação: Aquisição de Licença de software para monitoramento e proteção de dados sensíveis, incluindo análise comportamental de usuários, para ambiente on-premise WINDOWS OU LINUX E NAS (Network Attached Storage), com fundamento na Estratégia Nacional de Cibersegurança TSE/TREs 2021-2024. • Unidade de medida: usuários ativos no Active Directory (AD). • Natureza do objeto: Licença de Software • Justificativa da quantidade: A quantidade a ser registrada correspondente à quantidade de estimada de usuários cadastrados no Active Directory (AD).
2	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES, COM PAGAMENTODE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇA DE SOFTWARE, BENS INTANGÍVEIS	11.811	• Justificativa da contratação: Licença de software para monitoramento e proteção de dados, incluindo análise comportamental de usuários para Microsoft Exchange, para ambiente on premise ou em nuvem, com fundamento na Estratégia Nacional de Cibersegurança TSE/TREs 2021-2024. • Unidade de medida: usuários ativos no Serviço de E-mail (MS Exchange). • Natureza do objeto: Licença de Software • Justificativa da quantidade: A quantidade a ser registrada corresponde ao número de caixas postais por usuários registrados para a solução de E-mail MICROSOFT EXCHANGE ON PREMISE ou ON LINE.

3	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	LICENÇA DE SOFTWARE, BENS INTANGÍVEIS	30.536	• Justificativa da contratação: Aquisição de Licença de software para monitoramento e proteção de dados sensíveis, incluindo análise comportamental de usuários, para ambiente em nuvem (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3), com fundamento na Estratégia Nacional de Cibersegurança TSE/TREs 2021-2024. • Unidade de medida: usuários ativos na nuvem do Contratante. Natureza do objeto: Licença de Software • Justificativa da quantidade: A quantidade a ser registrada correspondente à quantidade de usuários do Contratante cadastrados no serviço de comunicação e colaboração em nuvem.
4	SERVIÇO DE INSTALAÇÃO, IMPLANTAÇÃO, PARAMETRIZAÇÃO E OPERACIONALIZAÇÃO	SERVIÇO	22	• Justificativa da contratação: Serviço de implantação correspondente à instalação e configuração da solução contratada. Deve ser registrado apenas 1(uma) unidade para cada Regional Partícipe. • Unidade de medida: Serviço. • Justificativa da quantidade: corresponde a implantação e configuração do conjunto de serviços contratados.
5	TREINAMENTO OFICIAL, NA FORMA REMOTA (ONLINE), COM DURAÇÃO DE 20 HORAS. (ATÉ 10 PARTICIPANTES)	TURMA	22	• Justificativa da contratação: Treinamento Oficial para a solução implantada visando a capacitação de técnicos do Tribunal. Corresponde a 1(uma) turma de até 10(dez) participantes. O Treinamento deverá cobrir conhecimentos necessários e habilidades para instalar, configurar, gerenciar, otimizar, resolver problemas e oferecer suporte à solução. • Unidade de medida: Turma. • Justificativa da quantidade: corresponde a 1 (uma) turma necessária para transferência de conhecimento por meio de treinamento oficial oficial na forma remota.
6	SERVIÇO DE APOIO OPERACIONAL, INVESTIGAÇÃO E ANÁLISE DE ALERTAS E COMPORTAMENTOS SUSPEITOS, POR 24 MESES, COM PAGAMENTO MENSAL.	UNIDADE	22	• Justificativa da contratação: O Serviço de operação assistida corresponde ao suporte continuado à solução fornecida pela contratada, visando auxiliar o contratante na análise de eventos de segurança. • Unidade de medida: Unidade - 24 meses, • Justificativa da quantidade: a quantidade corresponde a 1(uma) unidade referente a 24(vinte e quatro) meses, que cobre todo o período de garantia do fabricante para a solução, devendo possuir previsão de prorrogação na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

5. ESTIMATIVA DAS QUANTIDADES A SEREM CONTRATADAS (obrigatório)

Fundamentação: estimativa das quantidades a serem contratadas, acompanhada das memórias de cálculo e dos documentos que lhe dão suporte, considerando a interdependência com outras contratações, de modo a possibilitar economia de escala (inciso IV do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso V da IN 58/2022).

5.1. Todos os itens abaixo irão compor o objeto e deverão atender às especificações definidas nos requisitos técnicos deste Estudo Preliminar, de acordo com os quantitativos abaixo relacionados ao ambiente tecnológico da Justiça Eleitoral:

CONTRATAÇÃO NO FORMATO DE SERVIÇO, COM FORNECIMENTO DE SOLUÇÃO DE AUDITORIA, PROTEÇÃO DE DADOS, DETECÇÃO E RESPOSTA A AMEAÇAS A DADOS NÃO ESTRUTURADOS E METADADOS, ANÁLISE DE DADOS EM REPOSITÓRIOS CORPORATIVOS INTERNOS (ON PREMISES) OU NA NUVEM EM PLATAFORMAS DE COLABORAÇÃO, INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO E OPERACIONALIZAÇÃO, ALÉM DE SUPORTE TÉCNICO E SERVIÇO DE APOIO OPERACIONAL PELO PERÍODO DE 24 MESES, E TREINAMENTO PARA AS EQUIPES DO TRIBUNAL REGIONAL ELEITORAL DO PARÁ E TRIBUNAIS PARTÍCIPES.			
PRAZO DA CONTRATAÇÃO: 24 MESES			
ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE
1	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	38.396

2	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES, COM PAGAMENTODE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	11.811
3	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	30.536
4	SERVIÇO DE INSTALAÇÃO, IMPLANTAÇÃO, PARAMETRIZAÇÃO E OPERACIONALIZAÇÃO	SERVIÇO	22
5	TREINAMENTO OFICIAL, NA FORMA REMOTA (ONLINE), COM DURAÇÃO DE 20 HORAS. (ATÉ 10 PARTICIPANTES)	TURMA	22
6	SERVIÇO DE APOIO OPERACIONAL, INVESTIGAÇÃO E ANÁLISE DE ALERTAS E COMPORTAMENTOS SUSPEITOS, POR 24 MESES, COM PAGAMENTO MENSAL.	UND	22

Tabela - Bens e serviços de compõe a o objeto da contratação

5.3. Para o correto dimensionamento da solução, neste ETP foram considerados os seguintes quantitativos de infraestrutura do TRE-PA:

ITEM	DESCRIÇÃO	QUANTIDADE
1	**Quantidade de usuários de TI cadastrados no Active Directory** *Descrição: esse item deve contabilizar as contas/credenciais de usuários TI, por exemplo, magistradas(os), servidoras(es), colaboradoras(es) e estagiárias(os); assim como a quantidade de usuários de Sistemas e Serviços que utilizam o Active Directory como base para gerenciamento de credenciais.* ** O TRE-PA possui um total de:* *_ contas de usuários de TI cadastradas no Active Directory: 1.380* *_ contas de Sistemas e Serviços cadastrados no Active Directory: 100*	1.480
2	**Quantidade de usuários que utilizam o Microsoft Exchange *on premise* ou online** *Descrição: esse item deve contabilizar as contas/credenciais de usuários de TI que utilizam a solução de E-mail Microsoft Exchange on premise ou online.* ** O TRE-PA não utiliza em seu ambiente a solução de E-mail Microsoft Exchange, por esse motivo, foi informada a quantidade 0 (zero) para este item. Entretanto, este item foi incluído no projeto em razão da inclusão de Regionais partícipes na contratação conjunta que possuem esta solução implantada (vide tabela do ITEM 13.1 deste ETP).*	0
3	**Quantidade de usuários para ambiente de nuvem corporativa** *Descrição: esse item deve contabilizar a quantidade de usuários de TI que utilizam o ambiente de nuvem (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3)*	1.380

6. ESTIMATIVA DO VALOR DA CONTRATAÇÃO (obrigatório)

Fundamentação: estimativa do valor da contratação, acompanhada dos preços unitários referenciais, das memórias de cálculo e dos documentos que lhe dão suporte, que poderão constar de anexo classificado, se a Administração optar por preservar o seu sigilo até a conclusão da licitação (inciso VI do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso VI da IN 58/2022).

6.1. ANÁLISE DOS CUSTOS TOTAIS DA DEMANDA

6.1.1. Com base nos exemplos de contratação públicas similares, constam junto a cada contratação o valor contratado, que servirão como apoio para estimativa dos preços.

6.1.2. Cabe ressaltar que essas estimativas são baseadas nos serviços, volumetria e tempos de retenção pretendidos por cada órgão, não sendo exatamente o que foi quantificado pelo TRE-PA.

6.1.3. Desta forma, para se ter uma estimativa de custos mais efetiva e de acordo as necessidades e requisitos mencionados neste Estudo Preliminar, é mandatório que sejam feitas consultas a potenciais fornecedores para composição final de preços, após a escolha da solução indicada pela equipe de planejamento da contratação ter sido aprovada pela autoridade competente. O valor estimado final será fornecido após a pesquisa de preços pela unidade competente.

GRUPO 1 - SOLUÇÃO DE PROTEÇÃO, GESTÃO, MONITORAÇÃO DE DADOS NÃO ESTRUTURADOS					
ITEM	DESCRIÇÃO	UNIDADE DE MEDIDA	QUANTIDADE	VALOR ESTIMADO 24 MESES	VALOR TOTAL ESTIMADO
1	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	1.480	R$ 3.009,55	R$ 4.454.138,93
2	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES, COM PAGAMENTODE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	0	R$ 1.018,67	R$0,00
3	LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	USUÁRIOS	1.380	R$ 1.251,33	R$ 1.726.840,00

4	SERVIÇO DE INSTALAÇÃO, IMPLANTAÇÃO, PARAMETRIZAÇÃO E OPERACIONALIZAÇÃO	SERVIÇO	1	R$ 53.840,00	R$ 53.840,00
5	TREINAMENTO OFICIAL, NA FORMA REMOTA (ONLINE), COM DURAÇÃO DE 20 HORAS. (ATÉ 10 PARTICIPANTES)	TURMA	1	R$ 47.966,67	R$ 47.966,67
6	SERVIÇO DE APOIO OPERACIONAL, INVESTIGAÇÃO E ANÁLISE DE ALERTAS E COMPORTAMENTOS SUSPEITOS, POR 24 MESES, COM PAGAMENTO MENSAL.	24 MESES	1	R$ 10.529,00	R$ 252.696,00
VALOR GLOBAL ESTIMADO DA CONTRATAÇÃO					R$ 6.535.481,60

Tabela 1 - Bens e serviços de compõe a o objeto da contratação

Referência de valores:

- Pregão Eletrônico Nº 001/2023 - SECRETARIA DE ESTADO DE PLANEJAMENTO, ORÇAMENTO E ADMINISTRAÇÃO DO DISTRITO FEDERAL.
- Pregão Eletrônico Nº 17/2021 - AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA - ANEEL
- Pregão Eletrônico 5/2021 - TRIBUNAL DE CONTAS DO ESTADO DO ALAGOAS
- Pregão Eletrônico Nº 11/2022 - COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR - CAPES
- Pregão Eletrônico Nº 28/2019 - AGÊNCIA NACIONAL DE AVIAÇÃO CIVIL - ANAC
- Pregão Eletrônico Nº 058/2021 - TRIBUNAL SUPERIOR DO TRABALHO

7. JUSTIFICATIVAS PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO (obrigatório)

Fundamentação: Justificativas para o parcelamento ou não da solução. (inciso VIII do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso VII da IN 58/2022).

7.1. Justificativa para o agrupamento de itens.

7.1.1. O agrupamento dos itens do objeto do presente Instrumento em lote, tem por objetivo a padronização da contratação uma vez que os itens agrupados estão associadas a mesma solução tecnológica e possuem a mesma natureza técnica, o que resulta ainda na otimização de recursos humanos e financeiros no desenvolvimento das atividades relacionadas à gestão contratual, uma vez que o gerenciamento de número variado de fornecedores traz ineficiência e custo na gestão e fiscalização da contratação.

7.1.2. Além disso, em razão da complexidade da solução, a possibilidade do parcelamento torna o contrato técnica, econômica e administrativamente inviável ou provoca a perda de economia de escala. Neste sentido, justifica-se o agrupamento em lote, uma vez que entendemos ser a opção mais vantajosa à administração e satisfatória do ponto de vista da eficiência técnica, por manter a qualidade do projeto, haja vista que o gerenciamento e execução técnica permanece todo o tempo a cargo de um mesmo fornecedor.

7.1.3. De outro lado, justifica-se a adoção do agrupamento em lote em razão da interoperabilidade de componentes que fazem parte da solução, visando assegurar a integração e compatibilidade entre diferentes sistemas e plataformas, sem a necessidade de integrações de diferentes fornecedores. Ao agrupar a aquisição de softwares em um único lote, busca-se não apenas otimizar recursos financeiros e administrativos, mas também garantir uma abordagem coordenada que permita a criação de soluções e que entreguem resultados de forma sinérgica. Essa estratégia proporciona um ambiente propício para o desenvolvimento de sistemas que se complementam, facilitam a troca de dados e informações, reduzem redundâncias e, por consequência, promovem maior agilidade operacional e eficácia nos processos internos do órgão contratante.

7.1.4. Nesse diapasão, as vantagens seriam o maior nível de controle pela Administração na execução da prestação de serviços, a maior facilidade no cumprimento do cronograma preestabelecido, a observância dos prazos de entrega do objeto, concentração da responsabilidade pela execução a cargo de um fornecedor e melhor garantia no acompanhamento dos resultados, para o objeto estabelecido neste Termo de Referência.

7.1.5. Isto posto, o agrupamento em lote visa garantir a compatibilidade técnica e operacional entre os componentes da solução, visto que haverá integração entre software e hardware existente no TRE-PA, serviços prestados, a contratação será realizada através de um único lote.

7.2. Padronização.

7.2.1. Não é recomendável divisão em cotas para microempresas e empresas de pequeno porte, nos termos do art. 48, da Lei Complementar nº 123/2006; e do Decreto 8.538, de 6/10/2015, já que o tratamento diferenciado tem alto potencial de representar prejuízo ao conjunto do objeto a ser contratado, em face do princípio da padronização, descrito no Art. 47, I, da Lei nº 14.133/2021, que impõe a compatibilidade de especificações estéticas, técnicas ou de desempenho entre os itens, de maneira uniforme, observadas as condições de manutenção, assistência técnica e garantia oferecidas.

8. CONTRATAÇÕES CORRELATAS E/OU INTERDEPENDENTES

Fundamentação: contratações correlatas e/ou interdependentes (inciso XI do § 1° do art. 18 da Lei 14.133/21 e art. 9°, inciso VIII da IN 58/2022).

8.1. Não se faz necessária a realização de contratações correlatas e/ou interdependentes para a viabilidade e contratação desta demanda.

9. ALINHAMENTO DA CONTRATAÇÃO COM O PLANO DE CONTRATAÇÃO ANUAL(obrigatório) E PLANEJAMENTO ESTRATÉGICO

Fundamentação: demonstrativo da previsão da contratação no Plano de Contratações Anual, de modo a indicar o seu alinhamento com os instrumentos de planejamento do órgão ou entidade; (inciso II do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso IX da IN 58/2022).

9.1. O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme detalhamento a seguir:

I) PORTARIA TRE-PA Nº 21622/2022

II) Anexo IV - Serviços e bens de TIC

III) Item: 16

- Plano de Contratações 2023 - STI (Processo SEI Nº 0004285-30.2022.6.14.8000, evento 1723870)

10. DEMONSTRATIVO DOS RESULTADOS PRETENDIDOS

Fundamentação: demonstrativo dos resultados pretendidos, em termos de economicidade e de melhor aproveitamento dos recursos humanos, materiais e financeiros disponíveis (inciso IX do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso X da IN 58/2022).

- *Melhoria no gerenciamento dos dados e arquivos, quanto a classificação, propriedade, origem, consumo, restrições e volume (tamanho e quantidade);*
- *Melhoria na análise e classificação dos dados e arquivos, destacando-os como confidenciais, sensíveis, sigilosos e restritos, visando, principalmente, o atendimento a normativos com a Lei Geral de Proteção de Dados (LGPD);*
- *Realização de análise preventiva na manipulação e comportamento de arquivos e dados, buscando detectar, indicar e alertar quanto a anomalias, duplicações e possíveis ameaças;*

- *Detecção e alerta de acesso/uso indevido de dados e arquivos classificados como confidenciais, sensíveis, sigilosos e restritos, entre outras anomalias;*
- *Monitoramento de atividade dos usuários quanto ao acesso a dados e arquivos, registrando histórico de acesso;*
- *Capacitação da equipe para o melhor uso da Solução e seus módulos;*
- *Aumento do nível e maturidade na governança de dados;*
- *Fornecimento de uma camada extra de segurança da informação;*
- *Concretização das ações de segurança cibernética que visam proteger dados sensíveis e os ativos de informação dos Tribunais Regionais Eleitorais.*

11. PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Fundamentação: providências a serem adotadas pela Administração previamente à celebração do contrato (inciso X do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso XI da IN 58/2022).

A Equipe de Planejamento da Contratação apresenta a seguir as necessidades de recursos materiais e humanos, no que se refere à implantação, uso e à manutenção da Solução de TIC, para que o contrato possa ser devidamente executado e a solução de TIC atinja seus objetivos:

TIPO DE NECESSIDADE	UNIDADE RESPONSÁVEL	DESCRIÇÃO
Infraestrutura tecnológica	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Mudança ou Configuração	Unidade de Segurança Cibernética ou Seção de Segurança Cibernética	Auxílio na instalação de Máquinas Virtuais (VMs) que devem hospedar a solução e banco de dados da solução, implantação de conectores e configuração de ambiente.
Infraestrutura elétrica	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
obtenção de licenças	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Logística de implantação	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Espaço físico	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Mobiliário	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Impacto ambiental	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Capacitação fiscalização / gestão contratual	N/A	Nesse projeto, não há pendências relacionadas a este aspecto. Todo o ambiente está apto para a execução contratual.
Recursos Humanos	Fiscal técnico	*Gerenciar os aspectos técnicos da solução de auditoria*
	Gestor do contrato	*Atestar as faturas e realizar a fiscalização e gestão do contrato*

12. POSSÍVEIS IMPACTOS AMBIENTAIS E RESPECTIVAS MEDIDAS MITIGADORAS

Fundamentação: descrição de possíveis impactos ambientais e respectivas medidas mitigadoras, incluídos requisitos de baixo consumo de energia e de outros recursos, bem como logística reversa para desfazimento e reciclagem de bens e refugos, quando aplicável (inciso XII do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso XII da IN 58/2022).

12.1. Embora não se vislumbre nenhum tipo de impacto ambiental para a aquisição pretendida, devemos considerar as legislações vigentes que tratam do tema, e os efeitos relacionados ao desenvolvimento sustentável dos processos produtivos, sem contudo, comprometer a capacidade das gerações futuras em poderem dirimi-los de acordo com o seu tempo e carências, conciliando o desenvolvimento econômico com a preservação ambiental e bem-estar social;

12.2. A Contratada deverá obedecer os critérios de gestão ambiental estabelecidos nas normas, regulamentos e legislações federais, estaduais e municipais específicas visando a melhoria e o desempenho dos processos de trabalho quanto aos aspectos ambientais, sociais e econômicos;

12.3. Em relação o objeto da contratação em tela, percebe-se que o impacto da mesma ao meio ambiente é mínimo, uma vez que a entrega do software será realizada por meio digital (download), com instalação remota, mediante registro e aprovação do usuário, não havendo descarte de equipamento, embalagem ou qualquer outro resíduo.

13. ESTRATÉGIA DA CONTRATAÇÃO DO OBJETO

13.1. IRP - INTENÇÃO DE REGISTROS DE PREÇOS

A opção a seguir destaca a estratégia de contratação utilizada na Estratégia Nacional de Cibersegurança TSE e TREs (2021 a 2024), o qual permite a modalidade de compra conjunta em razão da necessidade de padronização de tecnologias, visando atender a arquitetura proposta na Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ).

( ) Pregão Eletrônico Tradicional

( ) Pregão Eletrônico - SRP

( ) Adesão a Ata de Registro de Preços*

(X) IRP (Intenção de Registro de Preços)

( ) Contratação Direta - **Inexigibilidade de Licitação** (Art. 74 e incisos da Lei 14.133/2021)

( ) Contratação Direta - **Dispensa de Licitação** (Art. 75 e incisos da Lei 14.133/2021)

O IRP é a manifestação prévia de um órgão público, informando sua intenção de participar do processo de registro de preços. A utilização do IRP (Intenção de Registro de Preços) traz várias vantagens como a economia em escala, uma vez que é possível obter melhores condições comerciais e preços mais vantajosos; além da flexibilidade e conveniência, pois cada órgão público possui a liberdade de utilizar o registro de preços de acordo com suas necessidades e disponibilidade orçamentária. Isso permite uma maior flexibilidade na contratação de bens ou serviços, conforme a demanda surgir, sem a necessidade de realizar uma nova licitação.

Visando o levantamento de informações entre os Tribunais Regionais Eleitorais interessados na contratação do objeto que trata este ETP, por meio do Ofício-Circular nº 5 / 2023 - TRE-DF/PR/DG/GDG, o Tribunal Regional Eleitoral do Distrito Federal - TRE/DF efetuou o levantamento de informações para dimensionamento de solução para auditoria de dados não estruturados, em atendimento ao previsto na Estratégia Nacional de Cibersegurança da Justiça Eleitoral para o ano de 2023. A referida consulta constitui do trabalho conjunto do TRE-DF e TRE-PA, objetivando conhecer a realidade de cada TRE, ante os requisitos tratados na elaboração dos Estudos Preliminares da Contratação. Como resultado deste Ofício-Circular, 23 Tribunais responderam a consulta, sendo que 20 demonstraram interesse em participar e enviaram suas respostas, e 03 responderam não ter interesse em participar.

Cumpre ainda salientar que, nos dias 30 e 31/05/2023 foi realizada no TSE o encontro de Secretários de TIC, no dia 30/05 especificamente, em uma das apresentações e discussões, os Secretários de TI do TRE-DF e TRE-PA em função do trabalho conjunto desenvolvido, acordaram que o TRE-DF apoiaria o referido projeto subsidiando as pesquisas junto aos TREs e revisando os artefatos da contratação e que o TRE-PA ficaria responsável pela realização da licitação.

Deste modo, para análise e posterior definição de solução que melhor atenda às necessidades e requisitos delineados neste Estudo Técnico Preliminar - ETP, foi realizado o levantamento de algumas informações para o dimensionamento de todos os itens essenciais que comporão a solução que será escolhida e ofertada a todos os Tribunais que demonstrarem interesse em participar desta contratação conjunta, conforme a seguir:

A) Qual a quantidade de usuários da rede de dados (servidores, terceirizados, prestadores de serviços,...) que tem login e senha de acesso a rede?

B) Qual a ferramenta utilizada como controlador do domínio, Active Directory da Microsoft ou outra baseada em LDAP?

C) Qual solução de colaboração é utilizada pelo Tribunal, Microsoft Teams ou Google Workspace?

D) O Tribunal utiliza servidores de arquivos on premises (interno), ou na nuvem? São Windows ou Linux, ou utiliza ambos?

E) O Tribunal utiliza serviço de correio eletrônico Microsoft Exchange? O serviço é on premises (interno), ou na nuvem?

A tabela a seguir consolida a resposta encaminhada (até 22/06/2023) pelos Tribunais Regionais Eleitorais que manifestaram interesse em participação na contratação (conforme encaminhado no evento 1933848):

CONSOLIDAÇÃO LEVANTAMENTO DE INFORMAÇÕES DOS TRIBUNAIS PARTÍCIPES

TRIBUNAL	QUANTIDADE DE USUÁRIOS	FERRAMENTA UTILIZADA COMO CONTROLADOR DE DOMÍNIO	SOLUÇÃO DE COLABORAÇÃO	SERVIDORES DE ARQUIVOS UTILIZADOS	UTILIZAM O EXCHANGE COMO SERVIÇO DE CORREIO ELETRÔNICO
TRE-DF	700	Active Directory (AD Microsoft)	Google Workspace	Google Workspace	Google Workspace
TRE-AM	1000	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise	Zimbra / on premise
TRE-AC	277	Active Directory (AD Microsoft)	Owncloud	Windows e Linux /On premise	Exchange / on premise
TRE-AP	325	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise	Exchange / nuvem
TRE-PR	3000	Active Directory (AD Microsoft)	Google Workspace	Google Workspace	Google Workspace
TRE-BA	2500	Active Directory (AD Microsoft)	Zoom	Windows / On premise	Zimbra / on premise
TRE-MG	4000	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise	Exchange / on premise
TRE-MT	936	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise	Exchange / nuvem
TRE-PA	1480	Active Directory (AD Microsoft)	Google Workspace	Windows / On premise e Google Workspace	Google Workspace
TRE-GO	2340	Active Directory (AD Microsoft)	N/A	Windows / On premise	Zimbra / on premise
TRE-SP	7019	Active Directory (AD Microsoft)	Google Workspace	Google Workspace / Unix TrueNAS	Google Workspace
TRE-MS	803	Active Directory (AD Microsoft)	N/A	Windows / On premise	Exchange / on premise
TRE-ES	1050	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise e Sharepoint nuvem	Exchange / Hibrido
TRE-PB	1512	Active Directory (AD Microsoft)	N/A	Windows e Linux /On premise	Zimbra / on premise
TRE-RJ	2373	Active Directory (AD Microsoft)	Google Workspace	Windows e Linux /On premise	Google Workspace
TRE-RS	1490	Active Directory (AD Microsoft)	Microsoft Teams	Windows Hibrido (On premises e nuvem)	Exchange / nuvem
TRE-MA	1500	Active Directory (AD Microsoft)	Google Workspace	Windows Hibrido (On premises e nuvem)	Não
TRE-TO	722	Active Directory (AD Microsoft)	Google Workspace	Google Workspace / Windows on premises	Google Workspace
TRE-PI	1500	Active Directory (AD Microsoft)	N/A	Windows e Linux /On premise	Não
TRE-CE	1792	Active Directory (AD Microsoft)	Microsoft Teams	Windows / On premise	Zimbra / on premise

Após nova consulta mediante Ofício-Circular nº 164 / 2023 - TRE/PRE/DG/STI/CGSI, para ratificação da quantidade correspondente aos TREs que manifestaram interesse, firam consolidadas as quantidades referentes aos itens da licitação, conforme quadro a seguir:

LOTE	ÓRGÃO (UASG)	QUANTIDADE POR ITEM					
		ITEM 1 - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT ACTIVE DIRECTORY, SERVIDORES DE ARQUIVOS ON PREMISE WINDOWS OU LINUX E NAS (Network Attached Storage) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.	**ITEM 2 - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS DO MICROSOFT EXCHANGE ON PREMISE OU ONLINE, POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.**	**ITEM 3 - LICENÇA DE USO, COM GARANTIA, DE SOFTWARE DE PROTEÇÃO DE DADOS SENSÍVEIS COM ANÁLISE COMPORTAMENTAL DE USUÁRIOS PARA AMBIENTE DE NUVEM (MICROSOFT SHAREPOINT ONLINE OU GOOGLE DRIVE OU AWS S3) POR 24 MESES, COM PAGAMENTO DE SUBSCRIÇÕES A CADA 12 MESES.**	**ITEM 4 - SERVIÇO DE INSTALAÇÃO, IMPLANTAÇÃO, PARAMETRIZAÇÃO E OPERACIONALIZAÇÃO (PARCELA ÚNICA)**	**ITEM 5 - TREINAMENTO OFICIAL, NA FORMA REMOTA (ONLINE), COM DURAÇÃO DE 20 HORAS, PARA ATÉ 10 PARTICIPANTES (PARCELA ÚNICA)**	**ITEM 6 - SERV APOIO OPERACIONA INVESTIGAÇ ANÁLISE DE ALERTAS E COMPORTAM SUSPEITOS, 2 (PAGAMENTO MENSAL)**
LOTE 1	TRE-AP / UASG 70029	325	325	325	1	1	1
	TRE-MG / UASG 70014	4.000	4.000	4.000	1	1	1
	TRE-MT / UASG 70022	963	963	963	1	1	1
	TRE-ES / UASG 70015	1.070	640	640	1	1	1
	TRE-RS / UASG 70021	1.490	1.490	1.490	1	1	1
	TRE-RO / UASG 70024	550	550	550	1	1	1
	TRE-AC / UASG 70002	277	277	---	1	1	1
	TRE-MS / UASG 70016	803	803	---	1	1	1
	TRE-DF / UASG 70025	700	---	700	1	1	1
	TRE-AM / UASG 70003	1.000	1000	1000	1	1	1
	TRE-PR / UASG 70019	3.000	---	3.000	1	1	1
	TRE-PA / UASG 70004	1.480	---	1.380	1	1	1
	TRE-SP / UASG 70018	7.200	---	7.850	1	1	1
	TRE-RJ / UASG 70017	2.373	---	2.373	1	1	1
	TRE-MA / UASG 70005	1.710	---	1.710	1	1	1
	TRE-TO / UASG 70027	1.000	---	1.000	1	1	1
	TRE-CE / UASG 70007	1.400	1.400	1.400	1	1	1
	TRE-BA / UASG 70013	2.500	---	--	1	1	1

	TRE-GO / UASG 70023	2.500	---	--	1	1	1
	TRE-PB / UASG 70009	1.800	---	--	1	1	1
	TRE-PI / UASG 70006	1.500	1500	1500	1	1	1
	TRE-RR / UASG 70028	500	400	400	1	1	1
	TOTAL	38.396	11.811	30.536	22	22	22

Tabela. Quantitativos a serem registrados

13.2. ESTRATÉGIA DE CONTINUIDADE DA SOLUÇÃO EM CASO DE INTERRUPÇÃO CONTRATUAL

Para que a execução contratual tenha continuidade deverá haver o monitoramento permanente do contrato, controlando as características normais e anômalas que possam comprometer a prestação dos serviços. As ações descritas a seguir deverão ser adotadas:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	AÇÕES DE CONTORNO	
				AÇÃO CORRETIVA E/OU PREVENTIVA RECOMENDADA	RESPONSÁVEL
Encerramento por abandono, inadimplemento ou incapacidade da empresa contratada	- Redução da capacidade de resposta a incidentes cibernéticos do órgão.	Empresa não ter comprometimento na execução do contrato	Aplicar sanção na empresa por descumprimento contratual	Acompanhar os prazos de entrega e monitorar a qualidade dos bens e serviços	Fiscal Técnico
		Falência da Empresa	Iniciar um novo processo administrativo visando uma nova contratação	Acompanhar a situação fiscal da empresa contratada	Fiscal Técnico e Administrativo
		Falta de capacidade/ qualificação da empresa na execução do contrato	Convocar o segundo colocado, quanto houver, do procedimento licitatório para assumir o contrato	Exigir atestados de capacidade técnica	Fiscal Técnico e Administrativo

13.3. ESTRATÉGIA DE INDEPENDÊNCIA DO TRE-PA COM RELAÇÃO A EMPRESA CONTRATADA

Uma vez contratado o objeto em questão, não será criado vínculo ou dependência de tecnologia exclusiva, permitindo este órgão buscar outros fornecedores no mercado. As ações descritas a seguir deverão ser adotadas:

EVENTO	EFEITO	CAUSAS	CONTROLES ATUAIS	AÇÕES DE CONTORNO	
				AÇÃO CORRETIVA E/OU PREVENTIVA RECOMENDADA	RESPONSÁVEL
Interrupção do fornecimento do licenciamento da solução, suporte/garantia e da prestação dos serviços	- Paralisação das atividades e do monitoramento, auditoria, classificação e proteção de dados. - Incapacidade de prevenção de ataques cibernéticos.	Desacordo contratual	Notificar a empresa acerca dos pontos de desacordo, visando sua melhoria	Gerenciar e monitorar a qualidade dos bens e serviços e os prazos de entrega	Fiscal Técnico
		Contenção de orçamento destinado ao contrato	Adotar novo modelo de contratação	Negociar com a empresa para diminuir o preço ou para fornecimento parcial	Fiscal Técnico e Administrativo
		Descontinuidade de oferta no mercado do serviço		Buscar a transição dos requisitos técnicos afetados para outras soluções disponíveis (ou complementares) no mercado	Fiscal Técnico e Administrativo

13.4. AÇÕES PARA TRANSIÇÃO CONTRATUAL

Os Fiscais Técnico e Administrativo deverão manter o monitoramento constante do contrato, visando mitigar ou controlar eventos que possam comprometer a execução contratual. As ações descritas a seguir serão adotadas no cenário de execução de transição contratual:

ID	AÇÃO	RESPONSÁVEL	INÍCIO	FIM
01	Realizar reunião inicial de alinhamento com a nova contratada sobre a execução do contrato	Gestor do Contrato e Empresa Contratada	Até 5 (cinco) dias corridos após a assinatura do contrato	Até a apresentação e aprovação de projeto de execução contratual
02	Apresentar o Projeto de Execução Contratual incluindo aspectos de repasse de conhecimento e outros assuntos afetos a continuidade do serviço	Empresa Contratada	Até 15 (quinze) dias corridos após a assinatura do contrato	Até a aprovação de projeto de execução contratual
03	Avaliar e aprovar o Projeto de Execução Contratual	Gestor do Contrato	Até 5 (cinco) dias corridos após apresentação e entrega do Projeto de Execução Contratual	Até o início do cumprimento do projeto de execução contratual
04	Iniciar o cumprimento do Projeto de Execução Contratual	Empresa Contratada sob supervisão do Gestor do Contrato com apoio do	Até 5 (cinco) dias corridos após a aprovação do Projeto de Execução	Até o fim do contrato

		Fiscal Técnico	Contratual	
05	Avaliar a execução do Projeto de Execução Contratual	Gestor do Contrato com apoio do Fiscal Técnico	Até 5 (cinco) dias corridos após o início do cumprimento do Projeto de Execução Contratual	Até o fim do contrato
06	Elaborar documento de aprovação formal do Projeto de Execução Contratual para dar continuidade na relação contratual	Fiscal Administrativo e Gestor do Contrato	Até 5 (cinco) dias corridos após a avaliação do Projeto de Execução Contratual	Após a avaliação do cumprimento do Plano de Execução Contratual

13.5. AÇÕES PARA ENCERRAMENTO CONTRATUAL

Ao longo do período de vigência da contratação, os Fiscais Técnico e Administrativo desempenharão ações de controle para o adequado encerramento do contrato, bem como poderá disponibilizar recursos para que a Contratada tenha condições de executá-lo, além de solicitar ações da Contratada para que haja condições de utilização do objeto de forma adequada após o encerramento. As ações de controle descritas a seguir serão adotadas:

Id	Ação	Responsável	Início	Fim
01	Validar a entrega das versões finais dos serviços e produtos alvos da contratação	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
02	Transferência final de conhecimentos sobre a execução e a manutenção da Solução de Tecnologia da Informação e Comunicação	Gestor do Contrato	Após a assinatura do contrato	Ao término do contrato
03	Devolução de recursos materiais	Não se aplica. Pela natureza do contrato, não há necessidade do TRE-PA disponibilizar recursos de TI para a contratada.	Após a assinatura do contrato	Ao término do contrato
04	Revogação de perfis de acesso	Haverá eventual necessidade de criação de perfis de acesso da contratada nas instalações de infraestrutura tecnológica do CONTRATANTE, em razão de acesso para instalação e configuração e serviço de apoio técnico e/ou mentoria. Deste modo, recomenda-se que o acesso remoto seja realizado por meio de solução de cofre de senha (PAM) ou VPN com recurso de 2FA habilitado	Após a assinatura do contrato	Ao término do contrato
05	Eliminação de caixas postais	Não se aplica. Não é necessário a criação de serviço postal para os funcionários da contratada.	Após a assinatura do contrato	Ao término do contrato
06	Realizar o encerramento administrativo do contrato	Gestor do Contrato	5 (cinco) dias antes do final do contrato	Ao término do contrato

13.6. DIREITOS DE PROPRIEDADE INTELECTUAL

13.6.1. Todas as informações, imagens e documentos a serem manuseados e utilizados são de propriedade do CONTRATANTE, não podendo ser repassadas, copiadas, alteradas ou absorvidas pela CONTRATADA sem expressa autorização da CONTRATANTE, de acordo com Termo de Compromisso de Manutenção de Sigilo e Termo de Ciência, a ser firmado entre a CONTRATADA e seus empregados, disponibilizada cópia à CONTRATANTE.

13.6.2. A CONTRATADA deverá entregar para o CONTRATANTE toda e qualquer documentação produzida decorrente da instalação da solução de TI, objeto desta CONTRATAÇÃO, bem como, cederá ao CONTRATANTE, em caráter definitivo e irrevogável, o direito patrimonial e a propriedade intelectual dos resultados produzidos durante a vigência do contrato e eventuais aditivos, entendendo-se por resultados quaisquer estudos, relatórios, especificações, descrições técnicas, protótipos, dados, bancos de dados, esquemas, plantas, desenhos, diagramas e documentação, em papel ou em qualquer forma ou mídia.

14. AVALIAÇÃO QUANTO À NECESSIDADE DE CLASSIFICAÇÃO DO ETP, NOS TERMOS DA LEI Nº 12.527/2011 (OBRIGATÓRIO)

Fundamentação: Art. 13 da IN SEGES 58/22 e 91, §1º, da Lei nº 14.133/2021.

14.1. Considerando não se tratar de licitação cujas informações nele constantes sejam sensíveis e imprescindíveis à segurança da sociedade e do Estado, não há necessidade de se atribuir qualquer tipo de classificação ao presente documento, nos termos dispostos na Lei nº 12.527/2011.

15. POSICIONAMENTO CONCLUSIVO SOBRE A VIABILIDADE E RAZOABILIDADE DA CONTRATAÇÃO (obrigatório)

Fundamentação: posicionamento conclusivo sobre a adequação da contratação para o atendimento da necessidade a que se destina. (inciso XIII do § 1° do art. 18 da Lei 14.133/2021 e Art. 9°, inciso XIII da IN 58/2022).

(X) Esta equipe de planejamento declara viável esta contratação com base neste Estudo Técnico Preliminar, consoante o Inciso XIII do art. 9º da IN 58, de 08 de agosto de 2022, - SEGES-ME.

( ) Esta equipe de planejamento declara inviável esta contratação com base neste Estudo Técnico Preliminar, consoante o Inciso XIII do art. 9º da IN 58, de 08 de agosto de 2022, - SEGES-ME.

Documento assinado eletronicamente por **CLEBER SOUSA FANJAS**, **Coordenador**, em 06/11/2023, às 12:15, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **CHARLES ALEX DOS SANTOS BATISTA**, **Assistente**, em 06/11/2023, às 12:16, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **ANTONIO EDIVALDO DE OLIVEIRA GASPAR**, **Coordenador**, em 06/11/2023, às 12:23, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **MARIA DO SOCORRO COIMBRA MOREIRA**, **Secretária Substituta**, em 06/11/2023, às 12:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

0000100-12.2023.6.14.8000 2037432v24