Tribunal Regional Eleitoral de São Paulo
ESTUDO TÉCNICO PRELIMINAR

Modelo v. 4.1

SEI nº 0058336-84.2024.6.26.8000

Aquisição de solução de cofre de senhas para a força de trabalho do TRE-SP

São Paulo - SP, 28 maio de 2025

ESTUDO TÉCNICO PRELIMINAR

INTRODUÇÃO

O Estudo Técnico Preliminar tem por objetivo identificar e analisar os cenários para o atendimento da demanda que consta no Documento de Oficialização da Demanda, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar o respectivo processo de contratação. É o documento que descreve as análises realizadas em relação às condições da contratação em termos de necessidades, requisitos, alternativas, escolhas, resultados pretendidos e demais características, e que demonstra a viabilidade técnica e econômica da contratação.

Referência: Guia de Contratações de TIC do Poder Judiciário (CNJ/ v. 4.0)

1 – IDENTIFICAÇÃO

Aquisição de solução de Cofre de Senhas para usuários do Tribunal Regional Eleitoral do Estado de São Paulo.

O Poder Judiciário, em destaque a Justiça Eleitoral, tem estabelecido diversos normativos acerca da adequação do ambiente de Tecnologia da Informação e Comunicação (TIC) ao novo cenário de transformação digital, buscando um ambiente tecnológico atualizado e seguro para a prestação de serviços com qualidade e eficiência para a população.

Dentre os normativos, destacam-se os seguintes:

I. Resolução TSE nº 23644/2021 que dispõe sobre a Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral;

II. Resolução CNJ nº 396/2021 que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ);

III. Resolução CNJ nº 370/2021 que estabelece a Estratégia Nacional de Tecnologia da Informação e Comunicação do Poder Judiciário (ENTIC-JUD);

IV. Resolução CNJ 468/2022 que 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.

A Resolução CNJ 396/2021, que estabelece a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-JUD), em seu capítulo 8, artigo 29, que trata sobre gestão de usuários elabora as seguintes determinações:

“Art. 29. Cada órgão do Poder Judiciário, com exceção do STF, deverá implementar a gestão de usuários de sistemas informatizados composta de:
I – gerenciamento de identidades;
II – gerenciamento de acessos; e
III – gerenciamento de privilégios.

Parágrafo único. A gestão de usuários será disciplinada por ato do Presidente do CNJ, que definirá o padrão a ser adotado para utilização de credenciais de login único e interface de interação dos sistemas, com o objetivo de uniformizar e garantir a experiência única de interação com os sistemas judiciais".

Além do cumprimento dos requisitos legais, é evidente o aumento constante de ataques cibernéticos direcionados a órgãos federais, especialmente aos componentes do Judiciário. Esses ataques têm como objetivo interromper a prestação de serviços à população, prejudicar o funcionamento das atividades institucionais e, muitas vezes, obter vantagens financeiras por meio do sequestro de dados críticos das organizações. Diante disso, torna-se essencial identificar e mitigar os riscos existentes, bem como implementar medidas eficazes de proteção contra esse tipo de ameaça.

Embora não seja possível garantir uma proteção total contra ataques cibernéticos, é viável reduzir significativamente os riscos por meio de estratégias eficazes. Entre elas, destacam-se a adoção de ferramentas para detectar e bloquear ameaças em tempo real, a proteção de contas com acessos privilegiados, bem como o uso de sistemas que assegurem o gerenciamento adequado de identidades e o controle de permissões de acesso.

Seguindo o definido na Estratégia Nacional de Segurança Cibernética, o TRE-SP adquiriu a solução de gestão de identidades e gerenciamento de acessos privilegiados da fabricante BeyondTrust, a qual se consolidou como um recurso essencial para a proteção do ambiente de TI.

A presente contratação decorre da necessidade do TRE-SP oferecer aos servidores que atuam neste Tribunal uma solução de cofre senhas para apoiar as boas práticas na gestão de senhas e atuar na redução de potencial risco passível de ser explorado por atacantes maliciosos.

2 – DEFINIÇÃO E ESPECIFICAÇÃO DAS NECESSIDADES E REQUISITOS

Identificação das necessidades de negócio

O Tribunal Regional Eleitoral do Estado de São Paulo (TRE-SP) investe continuamente em soluções de proteção do ambiente computacional, o que inclui as soluções de gestão de identidades, como exemplo, adquiriu a solução BeyondTrust como software de acesso privilegiado (PAM) conforme SEI 0014407-69.2022.6.26.8000, utilizada para proteger senhas e acessos à infraestrutura de TIC do TRE-SP.

No entanto, a solução adquirida atende apenas aos administradores do ambiente de TIC do Tribunal, tornando-se fundamental estender esse tipo de solução a todos os usuários de TIC do Tribunal, visando reduzir os riscos inerentes ao uso de senhas pela força de trabalho no acesso aos serviços e sistemas de uso rotineiro.

Entre as necessidades atendidas por esta solução se destacam as seguintes:

- Fortalecimento da segurança:

- facilitar a gestão de senhas fortes e únicas para as contas de usuários;
- reduzir a reutilização de senhas (uma prática comum e arriscada);

- armazenar senhas em ambiente protegido contra acessos não autorizados;

- Simplificação do gerenciamento de senhas:

- possibilitar à força de trabalho acessar várias contas e sistemas sem precisar lembrar de todas as credenciais; permitir o compartilhamento de senhas de forma segura entre equipes, eliminando o uso de métodos inseguros;

- Conformidade e auditoria:

- demonstrar maior maturidade em relação ao acesso a dados sensíveis;
- possibilitar o registro de acessos a credenciais, facilitando auditorias e eventuais investigações;

- Prevenção de incidentes:

- reduzir as chances de esquecimento de senhas, anotações em lugares inseguros ou compartilhamentos de forma inadequada;

- Produtividade:

- potencial redução de chamados relacionados a senhas esquecidas;
- eliminar a necessidade de procurar ou lembrar várias senhas.

Identificação das necessidades tecnológicas	
1	A solução ofertada deve permitir a autenticação por multifator (MFA) para evitar acessos não autorizados.
2	A solução deve permitir atribuição de permissões granulares, possibilitando que os usuários acessem apenas as senhas estritamente necessárias.
3	A solução deve utilizar funções de *hash* e algoritmos criptográficos fortes.
4	A solução deve realizar registro das atividades realizadas pelos usuários.
5	A solução deve permitir integrações com diretórios corporativos para facilitar o provisionamento e o desprovisionamento de usuários, garantindo alinhamento com a política de gestão de identidade da organização.
6	A solução deve permitir o compartilhamento controlado e seguro de credenciais entre usuários e equipes, sem exposição da senha em texto claro.
7	A solução deve permitir a rotação de senhas, caso desejado pelo usuário.
8	A solução deve oferecer suporte à plataforma Web, acesso por equipamentos móveis (tablet, smartphone) e uso em estações de trabalho e navegadores.
9	A solução deve possuir recurso para avaliar e alertar sobre o uso de senhas fracas ou vazadas.
10	A solução deve possuir alta disponibilidade e capacidade de recuperação das senhas em caso de falhas ou desastres, sem comprometer a segurança.

Demais requisitos necessários e suficientes à escolha da solução de TIC
Autorização do fabricante e Qualificação técnica

A presente contratação visa aquisição de solução tecnológica com suporte da licitante e garantia do fabricante da solução.

Assim, visando assegurar a idoneidade e a experiência da licitante na execução de contratos similares e objetivando a mitigação de riscos de inadimplemento contratual, falhas operacionais ou ineficiência técnica, deverá ser exigido atestado de qualificação técnica para verificar a capacidade da empresa para executar as atividades previstas no Termo de Referência.

Ainda, deverá ser solicitado documento que comprove a autorização formal da fabricante para que a licitante possa comercializar a solução ofertada, seja por meio de carta, declaração de parceria e/ou representação, sendo passível de verificação de legitimidade por parte do Tribunal.

Tal medida visa garantir que a licitante possua relação direta, legítima e autorizada com o fabricante da solução ofertada, detenha conhecimento das atualizações da solução, possua equipe capacitada para oferecer o suporte técnico e esteja apta a resolver eventuais demandas do Tribunal.

Demais requisitos necessários e suficientes à escolha da solução de TIC estão no Termo de Referência.

3 – ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Esta aquisição com escopo abrangendo toda a força de trabalho do Tribunal Regional Eleitoral do Estado de São Paulo é a primeira em execução por este TRE-SP, assim, para a definição de quantitativo de licenças necessárias para atendimento à demanda, foram requisitadas informações acerca do número de computadores ativos no Tribunal, quantidade de servidores (as) ativos (as), quantidade de magistrados(as), quantidade de estagiários(as) e quantidade de contratados (as) que utilizam um terminal computacional.

Após consulta às áreas do TRE-SP responsáveis pelos cadastros de Pessoal (doc 6497424), Magistrados (doc 6455676), Requisitados e Estagiários (doc 6497451), foram recebidos os quantitativos atuais e assim identificou-se que a solução deverá atender a um cenário que, hoje, possui um quantitativo de 3964 servidores, 407 magistrados, 1836 requisitados, 164 estagiários, o que totaliza 6307 possíveis usuários.

Entretanto, **considerando as variações no quantitativo de requisitados e estagiários, visando ainda a economicidade,** sugere-se a aquisição inicial de 6000 licenças para o TRE-SP, visando o atendimento à Resolução CNJ nº 396/2021, bem como à Portaria CNJ nº 140/2024.

4 – ANÁLISE DE SOLUÇÕES POSSÍVEIS

4.1 – IDENTIFICAÇÃO DAS SOLUÇÕES

Id	Descrição da solução (ou cenário)
1	BeyondTrust Workforce Passwords
2	CyberArk Workforce Identity Standard
3	Delinea Secret Server
4	Gestores de senhas individuais (gratuitos ou pagos)

4.2 – ANÁLISE COMPARATIVA DE SOLUÇÕES

Requisito	Solução	Sim	Não	Não se Aplica
A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública?	Solução 1	X		
	Solução 2	X		
	Solução 3		X	
	Solução 4			X
A Solução está disponível no Portal do Software Público Brasileiro? (quando se tratar de software)	Solução 1		X	
	Solução 2		X	
	Solução 3		X	
	Solução 4		X	
A Solução é composta por software livre ou software público? (quando se tratar de software)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões de governo ePing, eMag, ePWG?	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X
A Solução é aderente às orientações, premissas e especificações técnicas e funcionais do e-ARQ Brasil? (quando o objetivo da solução abranger documentos arquivísticos)	Solução 1			X
	Solução 2			X
	Solução 3			X
	Solução 4			X

4.3 – PESQUISA DE PREÇOS DE MERCADO

Id	Descrição da solução (ou cenário)
1	BeyondTrust Workforce Passwords (SaaS)
2	CyberArk Workforce Password Manager (SaaS)
3	Delinea Secret Server (SaaS)
4	Gestores de senhas individuais (gratuitos ou pagos)

5 – REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Durante os estudos técnicos preliminares foram elencadas soluções de uso individual (id 4) e soluções baseadas em *softwares* de mercado (id 1,2 e 3), entregues como serviço (SaaS).

Entretanto, permitir que os usuários utilizem gerenciadores de senhas individuais, sejam eles gratuitos ou pagos, por conta própria para o armazenamento de senhas corporativas traz alguns riscos de segurança e conformidade, entre os quais podemos citar:

- Falta de controle da organização
    - Permitir o uso de aplicativos pessoais pode causar impactos negativos quando uma pessoa sai da organização, pode comprometer a continuidade de serviços por falta de acesso a credenciais, etc.
    - Permitir que cada usuário escolha e use seu próprio gerenciador de senhas impossibilita a auditoria do uso da ferramenta pela organização;
- Despadronização
    - O uso não padronizado de uma solução para gerenciar senhas impossibilita a gestão do nível de segurança das diversas soluções possíveis;
- Desafios de conformidade:
    - O uso de soluções variadas impossibilita a organização validar se todas as ferramentas são aderentes à Política de Segurança da Informação do TRE-SP, se atendem aos normativos legais de proteção de dados, etc.

Soluções de gerenciadores de senhas de âmbito corporativo permitem integração com soluções de *Single Sign On* (SSO), bases de autenticação próprias, auditoria de atividades, imposição de políticas de senha, além do controle e revogação de acesso.

Sendo assim, o cenário que contempla a possibilidade de uso de gerenciadores de senhas individuais é incompatível ao atendimento dessa demanda e, portanto, torna-se inviável do ponto de vista técnico.

6 – ANÁLISE COMPARATIVA DE CUSTOS (TCO)

6.1 – CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE

BeyondTrust Workforce Passwords
Descrição:
Proposta doc (6498313) contempla subscrição da solução em nuvem para o período de 12 (doze) meses, incluindo serviço de instalação/configuração, bem como o serviço de suporte técnico pelo mesmo período. Proposta doc (6498327) contempla subscrição da solução em nuvem para o período de 36 (trinta e seis) meses, incluindo licenças e serviço de instalação/configuração e suporte técnico por 12 (doze) meses no primeiro ano. Nos outros dois anos contempla o custo da subscrição da solução em nuvem acrescido do suporte técnico por 12 (doze) meses a cada ano, totalizando 36 trinta e seis) meses.
Custo Total de Propriedade – Memória de Cálculo

BEYONDTRUST				
Cenário 12 meses - R$ 1.652.000,00				
Cenário 36 meses				
Ano	**Licença**	**Suporte**	**Implantação/ Treinamento**	**Total**
2025	R$ 1.530.000,00	R$ 72.000,00	R$ 50.000,00	R$ 1.652.000,00
2026	R$ 1.530.000,00	R$ 72.000,00	—	R$ 1.602.000,00
2027	R$ 1.530.000,00	R$ 72.000,00	—	R$ 1.602.000,00
			TOTAL	R$ 4.856.000,00

CyberArk Workforce Password Manager

Descrição:

Proposta doc (6502266) contempla subscrição da solução em nuvem para o período de 12 (doze) meses, incluindo serviço de instalação/configuração, bem como o serviço de suporte técnico pelo mesmo período.

Proposta doc (6505265) contempla subscrição da solução em nuvem para o período de 36 (trinta e seis) meses, incluindo licenças e serviço de instalação/configuração e suporte técnico por 12 (doze) meses no primeiro ano. Nos outros dois anos contempla o custo da subscrição da solução em nuvem acrescido do suporte técnico por 12 (doze) meses a cada ano, totalizando 36 (trinta e seis) meses.

Custo Total de Propriedade – Memória de Cálculo

CYBERARK				
Cenário 12 meses - R$ 1.073.885,96				
Cenário 36 meses				
Ano	**Licença**	**Suporte**	**Implantação/ Treinamento**	**Total**
2025	R$ 855.270,59	R$ 79.695,24	R$ 63.750,38	R$ 998.716,21
2026	R$ 855.270,59	R$ 79.695,24	—	R$ 934.965,83
2027	R$ 855.270,58	R$ 79.695,24	—	R$ 934.965,82
			TOTAL	R$ 2.868.647,86

Delinea Secret Server

Descrição:

Proposta doc (6498811) contempla subscrição da solução em nuvem para o período de 12 (doze) meses, incluindo serviço de instalação e configuração, bem como o serviço de suporte técnico pelo mesmo período.

Proposta doc (6498840) contempla subscrição da solução em nuvem para o período de 36 (trinta e seis) meses, incluindo licenças e serviço de instalação/configuração e suporte técnico por 12 (doze) meses no primeiro ano. Nos outros dois anos contempla o custo da subscrição da solução em nuvem acrescido do suporte técnico por 12 (doze) meses a cada ano, totalizando 36 (trinta e seis) meses.

Custo Total de Propriedade – Memória de Cálculo

DELINEA				
Cenário 12 meses - R$ 4.515.102,43				
Cenário 36 meses				
Ano	**Licença**	**Suporte**	**Implantação/ Treinamento**	**Total**
2025	R$ 4.164.292,67	R$ 72.000,00	R$ 140.000,00	4.376.292,67
2026	R$ 4.164.292,67	R$ 72.000,00	—	4.236.292,67
2027	R$ 4.164.292,67	R$ 72.000,00	—	4.236.292,67
			TOTAL	R$ 12.848.878,01

6.2 – MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Descrição da solução	Estimativa de TCO ao longo dos anos			Total
	Ano 1	Ano 2	Ano 3	
BeyondTrust Workforce Password	R$ 1.652.000,00	R$ 1.602.000,00	R$ 1.602.000,00	R$ 4.856.000,00
Cyberark Workforce Password	R$ 998.716,21	R$ 934.965,83	R$ 934.965,82	R$ 2.868.647,86
Delinea Secret Server	R$ 4.376.292,67	R$ 4.376.292,67	R$ 4.376.292,67	R$ 12.848.878,01

7 – DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Dentre as três soluções consideradas viáveis, todas atendem aos requisitos mínimos necessários para a contratação.

Em relação a possível vantagem econômica, conforme proposta da solução CyberArk (doc 6505265), realizando a contratação para um período de 36 (trinta e seis) meses, o valor total pode representar uma economia de **R$ 353.010,02** em relação à contratação por um período de 12 (doze) meses.

Com o intuito de maximizar os benefícios em contratações de maior prazo, e observando que, durante a realização do pregão, outros fornecedores podem apresentar propostas mais vantajosas financeiramente para um período de 36 (trinta e seis) meses, sugere-se a contratação de solução de cofre de senha para a força de trabalho do TRE-SP, na modalidade SaaS, com 6.000 (seis mil) licenças por 36 (trinta e seis) meses, passível de prorrogação, nos termos da Lei, contemplando implantação, garantia e suporte técnico durante a vigência contratual.

Essa aquisição busca uma gestão mais segura de credenciais pelos usuários de negócio do Tribunal e é um dos pilares da segurança da informação, especialmente diante do aumento de vetores de ataque que exploram credenciais privilegiadas, como phishing, credential stuffing e movimentações laterais em redes corporativas.

A contratação sugerida para 36 (trinta e seis) meses contribui diretamente para a evolução da maturidade do programa de segurança da informação, permitindo consolidar políticas e processos com estabilidade e previsibilidade.

Além disso, a implementação de uma solução de cofre de senhas eficaz requer fases como: configuração inicial da ferramenta (grupos, políticas, integrações, etc.) campanhas internas de sensibilização e treinamento com inclusão gradual das pessoas; por fim, com base no feedback dos usuários, ajustes devem ser realizados para que a solução atenda às expectativas e necessidades.

A adoção de uma solução de cofre de senhas exige mudança de comportamento por parte da força de trabalho, incluindo adaptação às boas práticas, compreensão da interface da ferramenta e incorporação do uso cotidiano em fluxos de trabalho, exigindo campanhas educativas regulares e suporte técnico contínuo.

Ainda, deve-se mitigar o risco de uma troca precoce de solução em ciclos curtos e interromper esse processo de aprendizado e internalização, que pode gerar resistência dos usuários diante de mudanças frequentes, perda de confiança na ferramenta, especialmente se interfaces ou funcionalidades mudam bruscamente, prejudicando assim a aderência às práticas seguras, pois usuários podem buscar atalhos inseguros frente a ferramentas mal compreendidas.

Portanto, visando reduzir o risco associado à descontinuidade e suas consequências, conforme descrito anteriormente, propõe-se uma contratação de 36 (trinta e seis) meses, com pagamento em parcelas anuais, não apenas para maximizar a eficiência econômica, mas também sustentar a evolução de segurança e o engajamento dos usuários do TRE-SP.

Critério de Sustentabilidade

Diferentemente de aquisições que envolvem bens físicos, consumo energético local, descarte de resíduos, materiais recicláveis, transporte ou embalagens, a contratação em pauta não implica movimentação logística, transporte terrestre ou aéreo de equipamentos; não envolve consumo de insumos físicos ou materiais, como papel, toner, embalagens ou componentes eletrônicos; não gera resíduos sólidos, químicos ou eletrônicos sob responsabilidade direta da CONTRATANTE e não prevê o fornecimento de hardware ou dispositivos, sendo o acesso remoto via dispositivos já existentes na organização.

Embora soluções SaaS possam, em tese, estar associadas a impactos indiretos relacionados à

infraestrutura de datacenters e consumo energético por parte do provedor, esses aspectos não são controláveis ou auditáveis diretamente pela contratante neste modelo de contratação. Além disso, os provedores de serviços em nuvem líderes de mercado já adotam políticas próprias de eficiência energética e sustentabilidade, como o uso de energia renovável, resfriamento inteligente e compensações de carbono, práticas que fogem do escopo direto de exigência contratual nesse caso específico.
A exigência de comprovações ambientais por parte do fornecedor poderia ser desproporcional ou irrelevante para o impacto real da contratação, e eventualmente restringir a competitividade de forma indevida.
Portanto, não foram encontrados critérios de sustentabilidade razoáveis ou aplicáveis à natureza do objeto contratado.

8 – ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

Com a análise dos valores coletados, considerando a razoabilidade dos valores e a adequação aos requisitos de negócio do TRE-SP, considerando ainda possíveis variações no custo devido ao prazo de contratação bem como ao modelo de pagamento anual. A estimativa resultante que representa um valor condizente com os preços praticados no mercado e que garanta uma contratação vantajosa para a Administração, encontra-se, neste momento, em R$ 2.868.647,86, conforme proposta referente à solução CyberArk (doc 6505265).

9 – SUSTENTAÇÃO E TRANSIÇÃO CONTRATUAL

Recursos necessários à continuidade do negócio durante a execução do contrato

O acompanhamento da execução contratual será realizado por servidores da SESEC – Seção de Segurança Cibernética.

A empresa contratada realizará reuniões periódicas, de forma remota, com o TRE-SP para acompanhamento do uso da ferramenta e resolução de eventuais dúvidas.

Continuidade contratual

Em caso de interrupção da prestação do serviço por parte da contratada, será necessário novo processo licitatório a ser conduzido pela SAM em conjunto com a área demandante, no menor prazo possível.

Transição contratual

Ao final do período de suporte, deve-se verificar a viabilidade de renovação do serviço.

Estratégia de independência

Esta contratação não prevê a produção ou desenvolvimento de software ou qualquer outro produto que caracterize propriedade intelectual.

10 – DECLARAÇÃO DE VIABILIDADE DA CONTRATAÇÃO

O presente ESTUDO TÉCNICO PRELIMINAR, elaborado pelos integrantes técnicos e administrativos, considerando a análise das alternativas, tendo em vista as necessidades tecnológicas e de negócio do TRE-SP, conclui-se pela viabilidade da aquisição da solução de cofre de senhas para a força de trabalho deste Tribunal, considerando os potenciais benefícios em termos de eficácia e no fortalecimento da segurança da informação institucional, melhoria na produtividade e maior capacidade de auditoria na gestão dos acessos.

11 – APROVAÇÃO E ASSINATURA

A Equipe de Planejamento da Contratação foi instituída pelo Documento de Oficialização da Demanda (doc. SEI 6376458), de 17 de fevereiro de 2025.

Marcio Rosostolato Machado *Integrante Técnico*	Rodrigo Moraes Barbosa *Integrante Demandante*	
Ana Beatriz Amorim Dantas *Integrante Administrativo*	Luciano Fernandes Leite *Integrante Administrativo*	
Equipe de Planejamento da Contratação		

Aprovo a viabilidade da Contratação.

Daniel Forlivesi
Titular da área Demandante