TRIBUNAL SUPERIOR ELEITORAL

ESTUDOS TÉCNICOS PRELIMINARES

I – Apresente a necessidade a ser atendida:

Proteger, controlar, gerenciar, auditar e monitorar contas privilegiadas a ativos críticos do Tribunal Superior Eleitoral.

São considerados ativos críticos: equipamentos servidores físicos e virtuais que hospedam todos os sistemas eleitorais, administrativos e judiciais; Servidores de Banco de Dados; Servidores de Arquivos Corporativos; Servidores de Correio Eletrônico do TSE, Equipamentos Firewalls, Banceadores de Carga, Switches de Rede, Proxy, Contas de Serviços, dentre outros.

II – Indique o público-alvo (unidades orgânicas, autoridades, servidores, outros) da contratação:

Servidores e colaboradores do TSE que fazem uso de contas que possuem acesso privilegiado para realizar a administração de ativos de Rede, Banco de Dados, Servidores de Aplicação.

O público alvo é composto dos servidores do quadro (Técnicos Judiciários e Analistas), assim como de Colaboradores que estão responsáveis pela administração de todos os ativos críticos citados acima. Todos os servidores e colaboradores atuam na STI. Alguns servidores ocupam cargo de gerenciamento da unidade (FC-6).

III – Indique a(s) consequência(s), caso não haja atendimento da necessidade:

Entre os fatores que influenciam os ataques cibernéticos, o furto de informações pessoais e o roubo de identidades está no topo da lista. De acordo com o relatório do Breach Level Index, desde 2016 este é considerado o principal tipo de violação de dados, com 59% do total das ocorrências do ano.

Desse modo, caso não seja atendida esta demanda o TSE estará vulnerável aos seguintes problemas, tais como:

1 - Acesso de várias pessoas utilizando a mesma conta, é impossível manter a trilha de auditoria, pois existem vários logins ao mesmo tempo. Há, também, a responsabilidade (accountability) mínima do uso da conta, e, como é compartilhada, muitas vezes as pessoas não se sentem responsáveis pela segurança e fazem coisas que não fariam com o seu próprio usuário, como escrever a senha em algum post-it.

2 -Falta de gestão da senha: Imagine mudar uma senha compartilhada por muitos. Isso requer que a senha seja distribuída de uma maneira segura. Isto pode significar mais trabalho, e propensão a erros, além possíveis falhas no tratamento destes.

3 - Vazamento de senhas de contas de usuários com privilégios de administrador;

4 - Ataques hackers: uma vez que tendo acesso a contas privilegiadas podem assumir o controle total de um sistema, roubando informações, alterando configurações, indisponibilizando serviços ou até mesmo destruindo de forma permanente informações importantes.

Por que proteger o acesso privilegiado?

As credenciais privilegiadas são os principais alvos de invasão dos cibercriminosos.

Uma conta privilegiada comprometida pode, por exemplo, conceder acesso irrestrito à infraestrutura de TI da Companhia, possibilitando ao atacante ter o controle administrativo das demais contas, obter dados internos sensíveis. Toda esta facilidade de acesso, fará com que os danos sejam irreparáveis para a empresa afetada.

Desta forma, busca-se uma solução que garanta a segurança operacional por meio de trilha de auditoria dos indivíduos que têm acesso a dados sensíveis ou processos críticos de TI.

IV – Indique o alinhamento da necessidade ao Planejamento Estratégico do TSE:

A presente contratação encontra-se alinhada ao Plano Estratégico do TSE 2018/2021, aprovado por meio da Resolução nº 23.567, de 17 de maio de 2018; Esta contratação também está alinhada aos objetivos do Planejamento Estratégico de Tecnologia da Informação e Comunicação (PETIC) do Tribunal Superior Eleitoral (TSE):

- Objetivo 1: Ampliar a segurança do processo eleitoral por meio de serviços e soluções de TI;
- Objetivo 3: Modernizar os serviços e as soluções de TI que suportam o processo eleitoral.
- Objetivo 7: Aprimorar as práticas e os controles de segurança da informação utilizados no desenvolvimento e na operação de serviços e de soluções de TI;
- Objetivo 8: Garantir a infraestrutura e os recursos tecnológicos adequados às atividades estratégicas do TSE;
- Objetivo 10: Aprimorar as práticas de governança de tecnologia da informação.

Atendimento ao constante no Art. 1º da Resolução 396 CN (1676014), Parágrafo Único.

Por fim, esta aquisição está em conformidade às iniciativas IN07.04 (nivelar infraestrutura à resolução 90 do CNJ):

IN07.E3 (prover a modernização dos serviços e recursos de TIC para adequação à dinâmica do negócio) do Plano Diretor de Tecnologia da Informação (PDTI), além de atender ao objetivo estratégico 7 (garantir a estrutura de TIC apropriada às atividades judiciais, eleitorais e administrativas).

V – Indique o resultado da pesquisa de mercado para identificação das soluções que possam atender às necessidades explicitadas:

LEVANTAMENTO DE ALTERNATIVAS DE SOLUÇÃO

1. **Solução 1**: Gestão de credenciais de forma manual e atualmente já existentes. É realizada por meio da utilização de planilhas ou textos armazenados em locais seguro e com controle de acesso às unidades envolvidas.
2. **Solução 2:** Software de gestores de senhas (carteiras de senhas) pessoais. Softwares utilizados para armazenar de forma segura senhas. Porém, cumpre apenas o papel de armazenamento seguro da credencial. Sem, no entanto, realizar o efetivo gerenciamento privilegiado aos equipamentos servidores, contas de serviços, servidores de banco de dados, etc...
3. **Solução 3**: Cofre de senhas, sistema que permite a gestão das credenciais privilegiadas, rotacionando as senhas periodicamente, controle o acesso a cada credencial.

Observação: A opção de utilização de **hardware de acesso** neste Estudo não foi considerada, haja vista que não existe a menor possibilidade de efetuar a gestão de senhas neste tipo de solução.

AVALIAÇÃO DAS ALTERNATIVAS DE SOLUÇÃO

Requisitos Desejáveis		Solução 1		Solução 2		Solução 3	
Descrição	**Peso**	**Avaliação**	**Nota**	**Avaliação**	**Nota**	**Avaliação**	**Nota**
• Eficiência	8	1	8	1	8	3	24
• Eficácia	8	1	8	1	8	3	24
• Economicidade	5	2	15	3	15	2	10
• Dependência de outras soluções	10	3	30	3	30	3	30
• Segurança	10	2	10	2	10	3	15
Nota Final		**71**		**71**		**103**	

- 0 - Não atende
- 1 – Atende precariamente
- 2 – Atende parcialmente
- 3 – Atende completamente

Alternativas	Quantidade	Preço Total (R$)
Solução 1	1	R$ 0,00 (sem custo) Porém, não supre os mínimos requisitos de segurança
Solução 2	1	R$ 20.000,00 (valor estimado) Porém, cumpre apenas o papel de armazenamento seguro da credencial. Não é possível realizar o efetivo gerenciamento privilegiado aos equipamentos servidores, contas de serviços, servidores de banco de dados, firewalls, balanceadores, etc...
Solução 3	1	**R$ 3.957.500,00**

REQUISITOS **(alíneas "a" a "e" do inciso II do art. 12 da IN 4/2014)**	**Solução**	**Sim**	**Não**	**Não se aplica**
• A Solução encontra-se implantada em outro órgão ou entidade da Administração Pública Federal?	1	x		
	2	x		
	3	x		
• A Solução está disponível no Portal do Software Público Brasileiro ?	1			x
	2		x	
	3		x	
• A Solução é um software livre ou software público?	1	x		
	2	x		
	3		x	
• Solução é aderente às políticas, premissas e especificações técnicas definidas pelos Padrões e-PING, eMAG?	1			x
	2			x
	3			x
• A Solução é aderente às regulamentações da ICP-Brasil? (quando houver necessidade de certificação digital)	1			x
	2			x
	3			x

JUSTIFICATIVA DA ESCOLHA DA SOLUÇÃO A CONTRATAR

De acordo com as soluções levantadas temos as seguintes considerações:

- A **solução 1 e 2** são inadequadas pois possui o menor grau de segurança, tornar inviável a auditoria sobre o uso das senhas, bem como não impede o vazamento das mesmas. Além disso fazer a rotação periódica de senha é algo inviável, pois implicaria na reconfiguração manual de sistemas aumentando o risco de indisponibilidades.
- **Na solução 3** as senhas são armazenadas no cofre e trocadas periodicamente sem que ninguém conheça tais senhas.

Outrossim, recomenda-se que haja permissão de adesão de outros órgãos à Ata de Registro de Preços com vistas a atender eventuais necessidades oriundas de Tribunais Regionais Eleitorais quanto à necessidade de aquisição desta mesma solução. Cabe ressaltar que esta medida vai ao encontro do que determina o Art. 1º da Resolução 396 CN (1676014), Parágrafo Único, assim como do que consta no Relatório - Estratégia Nacional de Cibersegurança v2 (1759818), pág. 14, na qual menciona a necessidade de aquisição de ferramentas automatizadas para governança e continuidade do negócio (Gestão de Acesso Privilegiado - (Cofre de Senhas).

PESQUISA DE PREÇO DE SOLUÇÃO DE COFRE DE SENHAS:

ITEM	DESCRIÇÃO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Cofre de Senhas - licenças de uso perpétuas - para controle de acesso à dispositivos, com garantia de versionamento por 60 (sessenta) meses.	2500 Licenças	R$ 1.523,00	R$ 3.807.500,00
2	Serviço de Instalação, Configuração e Transferência de Conhecimento	01	R$ 150.000,00	R$ 150.000,00
VALOR TOTAL				**R$ 3.957.500,00**

VI – Indique a descrição completa da solução que, por entendimento do(s) signatário(s) deste documento, melhor atenderá à necessidade especificada neste documento:

Trata-se de contratação de empresa para fornecimento de solução de cofre de senhas, com capacidade de efetuar o gerenciamento de acessos privilegiados (Privileged Access Management PAM) a dispositivos, acrescido de serviços de configuração, instalação e transferência de conhecimento.

Dessa forma, este Objeto está assim dividido:

1 - Solução de Cofre de Senhas (software), com fornecimento de 2500 (duas mil e quinhentas) licenças para controle de acessos privilegiados a dispositivos (ativos críticos).

2 - Serviço de instalação, configuração e transferência de conhecimento para as equipes que utilizarão a solução.

Esta solução proverá ao TSE o gerenciamento de acessos privilegiados, o gerenciamento de privilégios mínimos, proteção às credenciais privilegiadas, autenticação transparente, múltiplos fatores de autenticação e adoção de provisionamento de acessos; geração de relatórios sobre eventos, otimização nas rotinas de identificação, detecção e análise de eventos e incidentes, armazenamento de registros de ativos de rede unificado, com auxílio à respostas e remediações de incidentes de segurança.

Devido a constante busca por melhoria dos controles internos, as instituições necessitam de um controle mais efetivo do acesso lógico ao Datacenter, incluindo o controle de atividades executadas por terceiros e a identificação proativa de segurança de possíveis ameaças internas (alvo de constantes casos de ataques cibernéticos atuais).

Além da justificativa de eficiência operacional das atividades e mudanças realizadas no datacenter, acrescenta-se uma maior inteligência de segurança no rastreamento das atividades e possível identificação de anormalidades.

Não há uma forma eficaz para auditar o uso de tais credenciais. Manter as senhas dessas credenciais de forma seguras é um desafio enorme pois existe uma rotatividade de pessoas (servidores, estagiários e terceirizados). Quando as pessoas deixam as seções nada impede que elas levem consigo as senhas das credenciais privilegiadas.

Mudar as senhas periodicamente é algo extremamente complexo e, em alguns casos, impossível de se fazer, pois alterar as senhas implicaria em modificações em sistemas/serviços, o que poderia impactar na sua disponibilidade. Alguns sistemas possuem as mesmas senhas há diversos anos. Um dos principais objetivos dos hackers é ter acesso a contas privilegiadas, uma vez que tendo acesso a tais credenciais podem assumir o controle total de um sistema, roubando informações, alterando configurações, indisponibilizando serviços ou até mesmo destruindo de forma permanente informações importantes.

Ataque (roubo) a credenciais privilegiadas é uma pratica bem-sucedida no meio hacker e um dos principais alvos de ataque. Proteger de forma eficaz as credenciais privilegiadas é crítico para as instituições protegerem seus ambientes e informações.

O que é acesso privilegiado?

Uma credencial é considerada como acesso privilegiado quando possui direitos para administrar outras contas; alterar, remover arquivos e programas; gerenciar contatos; conceder ou revogar o acesso de outros usuários a sistemas.

Por isto, parte crucial deste trabalho é fazer uma identificação destas contas (Discovery). Isto quer dizer, achar todas as contas que constam dentro do TSE, seu uso e a forma como se correlacionam.

Depois do levantamento, o próximo desafio será efetivar as boas práticas de governança e GRC recomendadas, como a troca de senhas, no mínimo, a cada 3 meses (o ideal é que sejam trocadas mensalmente).

Por outro lado, essa é uma atividade humanamente impossível, por 2 motivos: o volume destas contas e as implicações desconhecidas que isto acarretaria, incluindo a parada de sistemas. O que exige que soluções de "cofre de senha" tenham além da capacidade de identificar automaticamente as credenciais privilegiadas e rotacionar suas respectivas senhas, tenham a capacidade de monitorar os acessos realizados nos dispositivos, identificando com precisão todos os acessos, e de preferencia de forma totalmente transparente para o usuário final, isto é, sem exigir mudanças de console, ou instalação de componentes extras.

A prática real de mercado está longe de ser um "best practices", pois, além de ser deficiente, abre um espaço para espionagem e fraudes internas, sem contar o trabalho manual de execução: cofres físicos, envelopes, logs, cerimônias, senhas divididas e muitas vezes, até associar uma senha à uma pessoa a fim de acessar uma multiplicidade de sistemas de alto valor, que constitui um risco adicional.

A solução, comumente chamado de "cofre de senhas", é controlar e automatizar todas as senhas através de um sistema central e consolidado, em que as senhas são geradas e propagadas para os sistemas remotos (destino). Assim, tais senhas não são compartilhadas a todo o momento, e somente quando se faz necessário alguma intervenção (planejada ou não).

VII – Indique o(s) estudo(s) realizado(s) ou o(s) critério(s) adotado(s) para definir o cálculo e a quantidade da necessidade:

Serão gerenciadas as credenciais privilegiadas de Servidores do Quadro Efetivo do TSE e Colaboradores, todos lotados na STI.

O quantitativo estimado já dispõe de uma estimativa para acréscimo no futuro, cerca de 10% em cada produto citado abaixo. Dessa forma, como o projeto em questão trata-se de uma intenção de Registro de Preços para Aquisição da Solução de Cofre de Senhas para o TSE, a medida que novos ativos forem sendo inseridos, haverá também a necessidade de realizar novas adesões a esta ata.

Por fim, informo que estes quantitativos aumentam a medida em que novos serviços/ativos são inseridos na rede do TSE.

Os quantitativos estimados de ativos de rede, contas de serviço, contas de usuários e contas de banco de dados, estão descritos na tabela abaixo:

QUANTIDADE ESTIMADA:

Ativo	Quantidade
• Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	200
• Servidores: hipervisor VMWARE, VMs, Windows e Linux	2.100
• Instâncias de banco de dados Oracle, MS SQL	100
• Instâncias de aplicações/serviços corporativos/senhas hardcode	500
• Usuários com acesso à dispositivos geridos pela solução	100
Total Geral	2.500 licenças para controle de dispositivos

VIII – Indique se a solução eleita é divisível ou não, levando em consideração o mercado que a fornece:

A solução deverá funcionar integrada e ser fornecida por uma única empresa.

Desta forma, a solução é indivisível.

IX – Indique, entre outras, as restrições internas de caráter técnico, operacional, regulamentar, financeiro e orçamentário, que possam dificultar a implementação da solução eleita:

Não há restrição de caráter técnico e operacional para a implementação e uso da solução nas instalações do TSE.

Identificamos a necessidade de apresentação de atestado de capacidade técnica por parte da empresa a ser contratada, comprovando estreita relação de parceria com a fabricante.

Acerca dos critérios de sustentabilidade, o documento da SEGESA que balizou a definição foi o SEI 1388575.

- A contratada não deve possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo;
- A contratada, ou seus dirigentes, não deve ter sido condenada por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo.
- Priorização de apresentação de documentos em formato eletrônico.

Optou-se por retirar o PCMSO, visto que não faz sentido avaliar risco ocupacional para este tipo de contratação, haja vista que não terá mão-se-obra alocada no TSE, tampouco desenvolvimento contínuo de software. O objeto em questão trata-se de aquisição de solução de cofre de senhas com entrega imediata.

NECESSIDADES DE ADEQUAÇÃO DO AMBIENTE PARA EXECUÇÃO CONTRATUAL:

Disponibilização do ambiente redundante para virtualização da solução para a implementação da solução a ser contratada.

DECLARAÇÃO DA VIABILIDADE DA CONTRATAÇÃO

Com base nas informações levantadas ao longo do Plano da Contratação, entendemos que a solução proposta é viável e vantajosa para o TSE, elevando o nível de segurança dos sistemas informatizados.

JUSTIFICATIVA PARA O PARCELAMENTO OU NÃO DA SOLUÇÃO

Não se aplica.

ANÁLISE DE RISCOS:

O objetivo deste documento é proporcionar um artefato que possa prever o acontecimento de eventuais riscos, que podem afetar a programação do projeto ou a qualidade da documentação que estão sendo desenvolvidas. Este documento abordará uma estratégia para identificar se o risco está ocorrendo, e possui estratégia para minimizar o impacto do risco e um plano de contingência para lidar com o risco se este ocorrer.

RISCO 1

Descrição do risco:	Contratação frustrada.
Probabilidade:	Média
Dano Potencial:	Necessidade de efetuar a troca de senhas de todos os usuários, ativos de rede e credenciais dos sistemas.
Ação Preventiva e Responsável:	Solicitação de patrocínio para apoiar a realização da contratação. Responsável: STI
Ação de Contingência e Responsável:	Aceitação do risco e notificação à Presidência e usuários da Justiça Eleitoral quanto à possibilidade de vazamento de dados e ataques hackers. Orientar aos usuários para que não utilizem dispositivos externos. Responsável: COINF/TSE

RISCO 2

Descrição do risco:	Atraso no fornecimento das licenças.
Probabilidade:	Baixa
Dano Potencial:	Atraso na implementação do gerenciamento de senhas
Ação Preventiva e Responsável:	Acompanhamento da execução do contrato. Realização de reuniões de acompanhamento com a contratada. Responsável: Fiscais do contrato.
Ação de Contingência e Responsável:	Interceder junto à contratada a fim de priorizar a entrega das licenças. Responsável: Fiscais do contrato.

RISCO 3

Descrição do risco:	Empresa contratada não entregar as licenças do produto
Probabilidade:	Baixa
Dano Potencial:	Possibilidade de comprometimento e vazamento de senhas com privilégios administrativos.
Ação Preventiva e Responsável:	Acompanhamento rígido da execução do contrato /Responsável: Fiscal do contrato.
Ação de Contingência e Responsável:	Realização de nova contratação. Responsável: STI e SAD.

X – Indique o valor estimado para a contratação:

O valor estimado para essa contratação, com manutenção, garantia de versionamento por 60 (sessenta) meses é de R$ 3.957.500,00 (três milhões, novecentos e cinquenta e sete mil e quinhentos reais)

De toda forma, e no momento oportuno, uma nova cotação de preços será encaminhada pela unidade responsável.

XI – Aquisição anterior no TSE:

Processo nº:	O TSE nunca teve uma gestão de senhas administrativas
Fornecedor:	Não se aplica
Resultado da análise:	

XII – Apresente os indicadores para avaliar a economicidade, a eficácia e a efetividade:

Esta contratação visa :

Garantir os princípios da segurança da informação: confidencialidade, integridade, disponibilidade e autenticidade. A proteção das credenciais privilegiadas impacta diretamente cada um desses princípios.

Atender a Política de Segurança da Informação e termos de confidencialidade do TSE, bem como atender a lei de geral de proteção de dados pessoais – LGPD, nº 13.709/2018.

Atender os requisitos de criptografia exigidos pela GSI da presidência. (Instrução Normativa GSI/PR nº 3, de 06 de março de 2013).

Benefícios Pretendidos:

A solução de gerenciamento de identidades deve:

Registrar os eventos realizados nas sessões privilegiadas;

Prover de forma segura o armazenamento centralizado das credenciais e acesso dos ativos de rede em alta disponibilidade;

Suportar integração com os sistemas internos do TSE;

Registrar as ações realizadas em posse de conta privilegiada com possibilidade de gravação de sessão (gravação de telas);

Melhorar controle sobre a utilização de recursos privilegiados do ambiente computacional;

Obter o monitoramento das ações de servidores e terceirizados com o uso de credenciais privilegiadas;

Melhorar qualidade na prestação de informações na investigação de incidentes de segurança;

Rastrear o uso de contas privilegiadas no ambiente computacional;

Aprimorar a segurança da informação e comunicação do TSE; e

Permitir a exportação das credenciais e senhas em formato seguro.

XIII – Indicação orçamentária:

A despesa correrá por conta do Programa 20 GP, cuja disponibilidade será informada posteriormente pela Secretaria de Planejamento, Orçamento, Finanças e Contabilidade (SOF).

XIV – Observações:

Informamos que a referida contratação não se enquadra nas previsões do Decreto nº 7.174/2010 tendo em vista tratar-se de produto importado.

Data limite para formalização do Contrato: 31/12/2021

Equipe de Planejamento: Ivanildo Ferreira Gomes / Marcelo Carneiro Rodrigues / Critiano Moreira Andrade

XV – Assinatura do servidor ou da equipe de planejamento da contratação responsável pela elaboração deste documento:

IVANILDO FERREIRA GOMES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **13/09/2021, às 15:36**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

CRISTIANO MOREIRA ANDRADE
COORDENADOR(A)

Documento assinado eletronicamente em **13/09/2021, às 15:39**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

MARCELO CARNEIRO RODRIGUES
CHEFE DE SEÇÃO

Documento assinado eletronicamente em **13/09/2021, às 15:48**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

A autenticidade do documento pode ser conferida em https://sei.tse.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0&cv=1778912&crc=13AD11E2, informando, caso não preenchido, o código verificador **1778912** e o código CRC **13AD11E2.**