TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

EDITAL DE LICITAÇÃO TSE Nº 85/2021

MODALIDADE: PREGÃO

FORMA: ELETRÔNICA

1. OBJETO

1.1. Registro de preços para eventual aquisição de Solução de Gerenciamento de Acessos Privilegiados para dispositivos (ativos de rede, servidores físicos e virtuais e outros sistemas tecnológicos), com capacidade para armazenar, proteger, controlar, gerenciar, auditar e monitorar o acesso privilegiado incluindo serviço de instalação e transferência de conhecimento, consoante especificações, exigências e prazos constantes deste Termo de Referência.

2. JUSTIFICATIVA

2.1. A Secretaria de Tecnologia da Informação possui a incumbência de assegurar que os serviços de TIC sejam prestados de forma satisfatória, com a finalidade de garantir o Princípio da Eficiência, o qual aduz que a "atividade administrativa deve ser exercida com presteza, perfeição e rendimento funcional, exigindo resultados positivos para o serviço público e satisfatório atendimento das necessidades".

2.2. Assim, em função desse princípio, a Administração Pública possui o dever de planejar adequadamente suas aquisições e contratações, com vistas a buscar a melhor solução para o total atendimento do interesse que se busca satisfazer, através de processo licitatório que irá selecionar a proposta mais vantajosa para tal fim.

2.3. Neste sentido, a Secretaria de Tecnologia da Informação adota, dentre outros, o método de proteção em camadas. Por este motivo, esta contratação de Solução de Gerenciamento de Acessos Privilegiados tem como objetivo proteger o ambiente de servidores da Justiça Eleitoral.

2.4. Este método consiste em criar várias camadas de proteção distintas e complementares, sendo cada camada atuando de forma especializada em algum componente de segurança.

2.5. A Justiça Eleitoral possui um parque de servidores diversificado, extremamente numeroso e que necessita de proteção constante. O cerne da celeridade de suas atividades, sejam elas meio ou fim, baseia-se nos recursos de tecnologia da informação. Apesar de facilitadora, a tecnologia da informação inclui novos riscos às informações recebidas, armazenadas ou transmitidas, o que requer métodos adequados de proteção das informações.

2.6. Esta solução proverá ao contratante 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.

2.7. 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).

2.8. 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.

2.9. Não há uma forma eficaz para auditar o uso de tais credenciais. Manter as senhas dessas credenciais de forma segura 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 prática 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.

2.10. O que é acesso privilegiado?

2.11. 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.

2.12. Por que proteger o acesso privilegiado?

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

2.14. 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.

2.15. 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.

2.16. A aquisição da solução de segurança visa assegurar à Justiça Eleitoral gestão permanente do ambiente, independentemente da marca ou do produto que estará sendo utilizado como ferramenta.

2.17. A natureza desta contratação tem fundamento na Lei nº 10.520/2002, no Decreto 10.024/2019 e nos termos da Lei nº 8.666/1993.

2.18. É considerado comum, o bem ou serviço cuja especificação estabelecer padrão objetivo de desempenho e qualidade e for capaz de ser atendida por vários fornecedores, ainda que existam outras soluções disponíveis no mercado.

2.19. Cumpre ressaltar que o texto supracitado estabelece relação entre a especificação e o seu atendimento por vários fornecedores, fato que o mercado atende facilmente. O objeto deste termo possui padrões de desempenho e qualidade que podem ser objetivamente definidos em Edital por meio de descrições usuais.

2.20. Tais características são aderentes à norma acima citada, indicando o enquadramento da licitação na modalidade Pregão.

2.21. Busca-se com esta modalidade indicada exercer ao máximo o princípio da economicidade, qual seja este um dos pilares da Administração Pública, a busca pela contratação mais vantajosa e econômica, sem, contudo, ferir ao princípio da isonomia, uma vez que está mantida a oportunidade de participação de todas as interessadas.

2.22. Tendo em vista que a demanda em questão visa garantir a segurança, proteção, integridade e autenticidade das informações armazenadas nos servidores do parque computacional da Justiça Eleitoral, entende-se necessária a aquisição de solução de gerenciamento de acessos privilegiados para o Tribunal Superior Eleitoral.

2.23. Os demais motivos que levaram a presente contratação, as justificativas para solução adotada, as quantidades definidas e demais questões afetas a esse Termo de Referência foram apresentadas no Estudo Preliminar (SEI nº 1849909).

2.24. Isto posto, esta equipe técnica propõe a aquisição da solução contemplando serviços de instalação, configuração com garantia técnica pelo período de 60 (sessenta) meses e transferência de conhecimento.

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1. DESCRIÇÃO DAS LICENÇAS E SERVIÇOS A SEREM EXECUTADOS

3.1.1. As especificações técnicas dos itens a serem fornecidos estão contidas no **ANEXO I-I - ESPECIFICAÇÕES TÉCNICAS** deste Termo de Referência.

3.1.2. A licitante deverá encaminhar proposta de preços especificando o fabricante e o nome comercial do produto ofertado.

3.1.3. Caso o produto que estiver sendo ofertado não atenda integralmente a todos os itens do edital, poderá ser realizada a composição com softwares de outros fabricantes.

3.1.4. Não será aceita a utilização de software livre, software grátis e software de código aberto (open source) na composição da Solução de Gerenciamento de Acessos Privilegiados.

3.1.5. A contratada será responsável pela integração e funcionamento das soluções utilizadas na composição, devendo garantir seu funcionamento durante toda a vigência da garantia.

4. CONDIÇÕES GERAIS

4.1. A instalação de qualquer componente fornecido neste objeto deverá prever a aplicação de todas as correções publicadas e divulgadas pelo fabricante, durante o prazo de garantia de 60 (sessenta) meses.

4.2. Para atender aos requisitos solicitados, caso sejam necessários componentes e/ou programas, cujas funcionalidades extrapolem o aqui especificado, estes deverão ser entregues conjuntamente com a solução fornecida, sem requerer licenças externas adicionais por parte do Contratante.

4.3. A Contratada será responsável por qualquer ônus decorrente de marcas, registros e patentes relativos ao fornecimento.

4.4. Para prestação da garantia técnica, a Contratada deverá sempre designar empregados qualificados e com a devida certificação técnica no produto. A fiscalização poderá exigir, a qualquer momento, que seja realizada o envio da certificação técnica, por e-mail, para a efetiva comprovação da qualificação do profissional. Caso a garantia técnica seja prestada pelo próprio fabricante, essa comprovação não será necessária.

4.5. A Contratada será responsável pela entrega das licenças no prazo máximo de 30 (trinta) dias corridos contados da notificação do contratante, após o início da vigência do contrato. As licenças deverão ser entregues em formato digital, por e-mail, ou para download em site do fabricante do produto.

4.6. Será permitido o uso de expressões técnicas de uso comum na língua inglesa.

4.7. As licenças devem ser de uso perpétuo, sem data de validade, e serem registradas em nome do contratante.

4.8. A instalação, configuração e transferência de conhecimento deverá ser concluída em até 30 (trinta) dias corridos contados da emissão do Termo de Recebimento Provisório das licenças.

4.9. Ao Tribunal Superior Eleitoral fica reservado o direito de recusar de pronto a solução que flagrantemente não esteja em conformidade com a especificação deste Termo de Referência.

5. RELAÇÃO ENTRE A DEMANDA PREVISTA E A QUANTIDADE DE CADA ITEM

5.10. Os quantitativos elencados neste Termo de Referência são provenientes de levantamento feito junto aos Tribunais Regionais Eleitorais - TREs e estão presentes no **Anexo I-VII - Quantitativos do TSE e TRE.**

5.11. Tem como motivo, ainda, o atendimento constante no Art. 1º da Resolução 396 CNJ (1676014), Parágrafo Único, assim como ao Relatório - Estratégia Nacional de Cibersegurança v2 (1759818), pág. 14, na qual consta a necessidade de aquisição de ferramentas automatizadas para governança e continuidade do negócio - Gestão de Acesso Privilegiado.

6. PARCELAMENTO DO OBJETO

6.1. A solução é composta dos seguintes itens:

Lote	Item	Descrição
ÚNICO	**1**	Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses.
	2	Serviço de Instalação, Configuração e Transferência de Conhecimento.

6.2. A adjudicação se dará para um único fornecedor.

7. GARANTIA TÉCNICA

7.1. A garantia técnica deverá ser prestada durante todo o período de validade da garantia técnica das licenças.

7.2. Os serviços de garantia pertinentes ao **Item 1** deverão ser realizados por técnicos do fabricante ou por técnicos da Contratada, certificados na solução.

7.3. Deverá ser executado nas modalidades remota e/ou presencial e englobar solução de problemas na ferramenta fornecida. A referida garantia técnica deverá ser prestada no regime 8x5 (oito horas por dia, cinco dias por semana), durante horário comercial, considerando o fuso horário do contratante.

7.4. O atendimento será realizado inicialmente de forma remota. Caso o problema tenha gerado indisponibilidade do ambiente e/ou não seja possível resolver de forma remota, o contratante poderá solicitar à contratada que o atendimento seja presencial.

7.5. O tempo máximo para início do atendimento a chamados é de 1 (uma) hora, contados da abertura do chamado junto à Contratada.

7.6. Os prazos referidos nos itens 7.3 e 7.4 são contabilizados de maneira contínua, ou seja, não são interrompidos em função do regime de atendimento 8x5 (oito horas por dia, cinco dias por semana). Uma vez aberto o chamado, deverão ser observados os prazos de atendimento e solução. A critério do contratante, poderá ser solicitado que o atendimento seja interrompido e tenha continuidade no próximo dia útil.

7.7. O tempo máximo para implementação de solução definitiva ou de contorno para problemas é de 6 (seis) horas, contados da abertura do chamado.

7.8. Caso o problema seja bug da ferramenta, deverá ser implementada uma solução de contorno e o prazo para solução definitiva deverá ser acordado com o contratante.

7.9. Caso o problema seja resolvido por meio do upgrade de versão da solução, ou instalação de patches, a Contratada deverá executar tal serviço em data e prazo acordados com o contratante.

7.10. A Contratada deverá analisar a instalação e configurações da solução, sempre que a equipe técnica do Contratante entender conveniente, para implementação de melhores práticas.

7.11. Sempre que houver incidentes relacionados à solução, o Contratante poderá solicitar à Contratada que realize ajustes na ferramenta.

7.12. As atualizações de software nos componentes e sistemas da solução poderão ser executadas remotamente, mediante autorização prévia do contratante.

7.13. Deverão ser fornecidas obrigatória e automaticamente todas as atualizações de versão que ocorrerem durante toda a vigência do período de garantia técnica das licenças.

7.14. A Contratada deverá executar o objeto deste Termo de Referência em conformidade com as determinações do fabricante da solução, normas técnicas pertinentes, especificações constantes na proposta apresentada.

7.15. O atendimento remoto deverá ser prestado diretamente pelos profissionais da Contratada ou do fabricante, através da plataforma de suporte remoto em uso (indicada) pelo contratante.

8. CRONOGRAMA DE EXECUÇÃO

8.1. A Contratada deverá cumprir os eventos descritos na tabela a seguir, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam:

MARCO (dias corridos)	EVENTO	RESPONSÁVEL	CRITÉRIO DE ACEITE
D	Publicação do Contrato	Contratante e Contratada	Contrato assinado.
D+5	Reunião de Planejamento	Contratante e Contratada	Ata de reunião assinada.
D+30	Entrega das Licenças	Contratada	Emissão do Termo de Recebimento Provisório.
E	Recebimento Provisório das Licenças	Contratante	Parecer do Fiscal Técnico.
E + 30	Concluir instalação, configuração e transferência de conhecimento da solução à equipe Contratante	Contratada	Solução implantada e funcionando plenamente.

8.2. Caso a Contratada verifique a impossibilidade de cumprir o prazo de entrega estabelecido, deverá solicitar prorrogação do prazo, pelo menos, 15 (quinze) dias corridos antes do seu vencimento, devendo a fiscalização do contrato manifestar-se quanto à solicitação no prazo de 2 (dois) dias úteis. O pedido de prorrogação do prazo deverá conter:

8.2.1. Motivo para não cumprimento do prazo, devidamente comprovado, e o novo prazo previsto para entrega.

8.2.2. A comprovação de que trata esta cláusula deverá ser promovida não apenas pela alegação da Contratada, mas por meio de documentos que relatem e justifiquem a ocorrência que ensejará o descumprimento do prazo, tais como: carta do fabricante/fornecedor, laudo técnico de terceiros, Boletim de Ocorrência de Sinistro, ou outro equivalente.

9. RECEBIMENTO

9.1. Recebimento Provisório:

9.1.1. Para o Item 1: em até 2 (dois) dias úteis, contados do recebimento das licenças, será emitido o Termo de Recebimento Provisório - TRP, por servidor ou comissão previamente designados, ressalvadas as hipóteses do art. 74 da Lei 8.666/93.

9.1.2. Para o Item 2: em até 2 (dois) dias úteis, contados do fim da transferência de conhecimento, será emitido o Termo de Recebimento Provisório - TRP, por servidor ou comissão previamente designados, ressalvadas as hipóteses do art. 74 da Lei 8.666/93.

9.2. Após a emissão de cada TRP, o fiscal técnico ou comissão designada terão o prazo de até 5 (cinco) dias úteis, a contar da instalação das licenças, para emitir o respectivo Termo de Recebimento Definitivo - TRD e remeter o processo ao fiscal administrativo. O TRD compreenderá a verificação da conformidade do objeto executado por meio das análises e conclusões dos quesitos previstos na Lista de Verificação - Anexo I-III deste Termo de Referência.

9.2.1. No caso do item 1, a comprovação, junto ao fabricante, do registro das licenças em nome do contratante, prevista na Lista de Verificação, poderá ser feita por meio de consulta no site do fabricante.

9.2.2. Identificada qualquer irregularidade pela fiscalização durante o recebimento de cada item, a Contratada deverá saná-la no prazo de até 5 (cinco) dias corridos, contados da notificação.

9.2.3. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização, será reaberto novo prazo de 5 (cinco) dias úteis para emissão do TRD.

9.2.4. O TSE poderá rescindir a contratação caso o objeto entregue seja novamente reprovado.

9.2.5. Todas as evidências de descumprimento das obrigações assumidas, no todo ou em parte, pela Contratada constarão do TRD para viabilizar a apuração da importância exata a pagar.

9.2.6. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento em até 5 (cinco) dias úteis, contados do TRD.

9.2.7. A fiscalização que será realizada pelo contratante não exclui nem reduz a responsabilidade da Contratada, inclusive perante terceiros, por qualquer irregularidade, ainda que resultante de imperfeições técnicas ou vícios redibitórios, e, na ocorrência desta, não implica em corresponsabilidade da Administração, em conformidade com o art. 70 da Lei nº 8.666/93.

10. PAGAMENTO

10.1. O pagamento de cada item será efetuado até o 10º (décimo) dia útil, a partir do atesto da respectiva nota fiscal/fatura, pelo servidor responsável, com a emissão de ordem bancária para o crédito em conta corrente da contratada, observada a ordem cronológica estabelecida no art. 5º da Lei nº 8.666/93.

10.1.1. O atesto do objeto contratado se dará pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA, conforme previsto na IN nº 11/2021- TSE. O fiscal administrativo terá o prazo de 2 (dois) dias úteis para emitir a NTA e remeter o processo à CEOFI, contados do recebimento do documento fiscal, acompanhado do Termo de Recebimento Definitivo - TRD e dos demais documentos exigidos para liquidação e pagamento da despesa.

10.1.2. Na fase de liquidação e pagamento da despesa, a unidade de execução orçamentária e financeira realizará consulta *on-line* ao Sistema de Cadastramento Unificado de Fornecedores – SICAF, ou nos sítios de cada órgão regulador, com fins de verificar a regularidade da contratada perante a Seguridade Social e a Fazenda Federal, o Fundo de Garantia por Tempo de Serviço e a Justiça Trabalhista.

11. OBRIGAÇÕES DA CONTRATADA

11.1. Executar, com observação dos prazos e exigências, todas as obrigações constantes deste Termo de Referência.

11.2. Assinar o termo de confidencialidade disponível no Anexo I-V deste Termo de Referência por meio de seu preposto e todos os demais funcionários que forem atuar na execução da contratação.

11.3. Responsabilizar-se pelas despesas decorrentes da execução dos serviços objeto deste Termo de Referência.

11.4. Informar, no momento da assinatura do instrumento contratual, nome do responsável, os contatos de telefone, e-mail ou outro meio hábil para comunicação com o contratante, bem como manter os dados atualizados durante toda a fase de execução da contratação.

11.4.1. Toda a comunicação referente à execução do objeto será realizada através do e-mail informado pela Contratada no momento da assinatura do contrato ou por outro meio desde que previamente acordado entre as partes.

11.4.2. A comunicação será considerada recebida após a confirmação de entrega automática encaminhada por e-mail (Outlook), independentemente de confirmação de recebimento por parte da contratada, ficando sob sua responsabilidade a verificação da caixa de e-mail.

11.4.3. A comunicação só será realizada de forma diversa quando a legislação exigir ou quando a Contratada demonstrar ao fiscal os motivos que justifiquem a utilização de outra forma.

11.5. Acatar as recomendações efetuadas pelo fiscal do contrato.

11.6. Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto deste Termo de Referência.

11.7. Fornecer à fiscalização do contrato relação nominal, com os respectivos números de documento de identidade de todo o pessoal envolvido diretamente na execução dos serviços, em até 3 (três) dias úteis após a publicação do extrato do contrato no Diário Oficial da União, bem como informar durante toda a vigência qualquer alteração que venha a ocorrer na referida relação.

11.8. Fazer com que seus empregados se submetam aos regulamentos de segurança e disciplina durante o período de permanência nas dependências do contratante, não sendo permitido o acesso dos funcionários que estejam utilizando trajes sumários (shorts, chinelos de dedo, camisetas regatas ou sem camisa).

11.9. Comunicar ao contratante, por escrito, em um prazo de até 24 (vinte e quatro) horas, quando verificar condições inadequadas de execução do objeto ou a iminência de fatos que possam prejudicar a sua execução e prestar os esclarecimentos que forem solicitados pelos fiscais.

11.10. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo contratante, não os divulgando, copiando, fornecendo ou mencionando a terceiros e nem a quaisquer pessoas ligadas direta ou indiretamente à Contratada, durante e após a vigência do contrato, inclusive em relação aos dados de infraestrutura, arquitetura, organização e/ou qualquer outra informação relativa ao ambiente tecnológico ou procedimentos técnicos do contratante.

11.11. Manter, durante a execução do contrato, as condições de habilitação exigidas na licitação, quanto à regularidade fiscal.

11.12. Responsabilizar-se pelos encargos fiscais e comerciais resultantes desta contratação.

11.13. A inadimplência da Contratada com referência aos encargos suportados não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto do contrato.

11.14. Diante da Pandemia de Covid-19, em caso de atendimento presencial, a Contratada deverá:

11.14.1. Fornecer máscaras N95 aos seus funcionários, em quantidade suficiente, para ingresso e permanência nas dependências do contratante, em atenção aos protocolos sanitários observados pelo Contratante em decorrência da pandemia da COVID-19.

11.14.2. Orientar seus funcionários acerca da necessidade de observar protocolos sanitários definido pelo Contratante em decorrência da pandemia da COVID-19.

11.14.3. Afastar os funcionários que apresentarem sintomas da COVID-19, sem prejuízo da prestação dos serviços.

11.14.4. O Contratante poderá solicitar, a qualquer tempo, que o suporte seja realizado remotamente utilizando a ferramenta indicada pelo contratante, conforme item 7.14 do Capítulo 7 do Termo de Referência.

12. OBRIGAÇÕES DO CONTRATANTE

12.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela Contratada.

12.2. Acompanhar, fiscalizar e atestar a execução contratual, bem como indicar as ocorrências verificadas.

12.3. Designar servidor ou comissão de servidores para fiscalizar a execução do objeto contratual.

12.4. Permitir que os funcionários da Contratada, desde que devidamente identificados, tenham acesso aos locais de execução dos serviços.

12.5. Recusar qualquer serviço entregue em desacordo com as especificações constantes desse Termo de Referência ou com defeito.

12.6. Receber a Contratada para reunião inaugural, conforme prazo definido no item 8.1 (Cronograma de Execução).

12.7. Efetuar o pagamento à Contratada segundo as condições estabelecidas nesse Termo de Referência.

13. PRAZO DE VIGÊNCIA DO CONTRATO

13.1. O(s) contrato(s) oriundo(s) da ARP terá(ão) vigência a partir de ___ de _____ de 202__ e duração de 6 (seis) meses.

14. SUBCONTRATAÇÃO

14.1. É vedado à Contratada transferir a outrem a parcela de maior relevância do objeto deste Termo de Referência. Todavia, fica permitida a subcontratação do próprio fabricante, para execução dos serviços de garantia técnica.

15. CONSÓRCIO

15.1. É vedada a participação em consórcio.

15.2. Durante a elaboração deste Termo de Referência, foi constatada pela equipe técnica a existência de diferentes empresas que atendem aos requisitos mínimos (especificações e condições) e poderão participar do certame, de tal forma que a vedação à participação em consórcio não representa restrição à competição.

16. CRITÉRIOS DE SUSTENTABILIDADE

16.1. Comprovação de não possuir inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MM/IRDH nº 4/2016, a partir da verificação do nome da empresa em lista emitida pelo Ministério do Trabalho e Previdência, atualizada periodicamente em seu sítio eletrônico (https://www.gov.br/trabalho/pt-br/assuntos/fiscalizacao/combate-ao-trabalho-escravo).

16.2. Comprovação de não ter sido condenada, a licitante ou seus dirigentes, por infringir as leis de combate à discriminação de raça ou de gênero, ao trabalho infantil e ao trabalho escravo, em afronta ao que está previsto no art. 1° e no art. 170 da Constituição Federal de 1988; no art. 149 do Código Penal Brasileiro; no Decreto n° 5.017, de 12 de março de 2004, (promulga o Protocolo de Palermo) e nas Convenções da OIT, no art. 29 e no art. 105.

16.2.1. A comprovação deverá ser feita por meio de apresentação de Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa") **da Justiça Federal e da justiça comum** para a licitante e seus dirigentes.

16.3. Na especificação dos bens, adotou-se como medida sustentável a obrigação da Contratada de fornecer as licenças em meio digital.

17. PREÇOS ESTIMADOS

Lote	Item	Descrição	Unidade	Quantidade Inicial Estimada	Quantidade Total	Valor Unitário (R$)
ÚNICO	1	Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses.	Licenças	1.500	14.267	1.570,00
	2	Serviço de Instalação, Configuração e Transferência de Conhecimento.	Serviço	1	26	150.000,00

ANEXO I-I - ESPECIFICAÇÕES TÉCNICAS

18. ITEM 1 - SOLUÇÃO DE GERENCIAMENTO DE ACESSOS PRIVILEGIADOS

18.1. Auditoria e gerenciamento de acesso lógico por meio de credenciais privilegiadas para até 14.267 (quatorze mil, duzentos e sessenta e sete) dispositivos (ativos de rede e servidores físicos e virtuais de serviços e sistemas tecnológicos), distribuídos entre o Tribunal Superior Eleitoral e os Tribunais Regionais Eleitorais.

18.2. As soluções instaladas no Tribunal Superior Eleitoral e nos Tribunais Regionais Eleitorais devem funcionar de maneira completamente independente.

18.3. Para soluções que são licenciadas por usuários e não por dispositivos, deverá ser utilizado um fator de conversão de 10 usuários para cada 100 dispositivos.

18.3.1. Caso o número de usuários resultante seja fracionado, este deverá ser arredondado para cima.

18.4. A solução deve proteger contra a perda, roubo e gestão inadequada de credenciais através de regras de complexidade da senha que incluem comprimento da senha (quantidade de caracteres), frequência de troca da senha, especificação de caracteres permitidos ou proibidos na composição da senha e outras medidas.

18.5. A solução deve mitigar problemas de segurança relacionados ao compartilhamento de contas que são armazenadas localmente em dispositivos e também para as contas que não são gerenciadas de forma centralizada por serviços de diretórios.

18.6. A solução deve descobrir credenciais privilegiadas referenciadas por serviços e processos automatizados incluindo tarefas agendadas do Windows (Scheduled tasks) e Serviços Windows. Além disso, a solução deve propagar as senhas geradas de forma aleatória onde quer que estas estejam referenciadas;

18.7. A solução deve garantir a quantidade de acessos a sua interface conforme a necessidade do Contratante e não deve limitar o número de contas que podem ser gerenciadas em um alvo licenciado.

18.8. A solução deve suportar métodos de alta disponibilidade para todos os componentes que fazem parte da solução, a fim de mitigar riscos inerentes à indisponibilidade destes. A solução deve ainda contemplar a expansão, incremento ou melhoria exclusivamente destes métodos sem qualquer custo adicional de licenciamento da solução para o Contratante.

18.9. A solução deve atender o conceito de tolerância a falhas e não ter restrições para funcionar em modo de alta disponibilidade ativo – ativo ou ativo – passivo.

18.10. A solução deve suportar alta-disponibilidade ativo/passivo onde na falha do primário, o appliance ou servidor secundário deve assumir suas funções automaticamente permitindo a continuidade do acesso as contas privilegiadas.

18.11. O chaveamento do appliance/servidor primário para o appliance/servidor secundário deve ser feito por completo, incluindo funções primordiais como troca de senhas, gravação de sessões e etc.

18.12. Todas os controles de alta disponibilidade devem ser feitos via interface gráfica, sem depender de comandos manuais, scripts ou adaptações.

18.13. A sincronização de dados os servidores/appliances da solução deve ser gerenciada nativamente pela solução sem necessidade de intervenção manual para garantia de sincronia entre os dois appliances.

18.14. A solução deve utilizar um banco de dados não proprietário. O banco de dados deve permitir alta disponibilidade e mecanismos para a recuperação de desastres.

18.15. A ferramenta deverá permitir o backup e recovery de seu banco de dados, bem como das configurações de software estabelecidas, com as seguintes capacidades:

18.15.1. Deverá permitir a execução de backups sem paradas do sistema;

18.15.2. Deverá permitir a execução de backups automatizados, permitindo a sua programação/agendamento;

18.16. A solução não deve utilizar qualquer tipo de agente, sejam eles nas consoles de gerenciamentos, dispositivos alvos ou em qualquer outro componente que faça parte da solução.

18.17. A solução deverá ser entregue em formato de appliance virtual para execução em máquinas físicas ou virtuais, virtualizadas sob a plataforma VMware, na versão 7.0.

18.18. Serão aceitas soluções entregues em software, desde que todos os componentes necessários para seu funcionamento (como sistema operacional, banco de dados e licenças adicionais necessárias) sejam contemplados na proposta e entrega da solução.

18.19. A solução deve possuir um dashboard ou método similar, que possa demonstrar a saúde da solução através de dados como utilização de disco, CPU, memória, serviços em execução, serviços parados e gráficos que demonstrem o uso de CPU.

18.20. A solução deve suportar a geração notificações por e-mail e/ou SNMP no caso em que os serviços essenciais sejam parados e/ou se problemas no hardware forem detectados.

18.21. A solução deve possibilitar a utilização de criptografia do banco de dados utilizado pela solução para armazenar as senhas das credenciais gerenciadas pela mesma. Deve ainda ser compatível com os seguintes métodos de criptografia:

18.21.1. AES com chaves de 256 bits

18.21.2. FIPS 140-2

18.22. Suportar utilização de hardwares de HSM através de PKCS#11 ou superior.

18.23. Incorporar medidas de segurança, incluindo criptografia, a fim de proteger a informação em trânsito entre os módulos distribuídos e entre as aplicações Web dos usuários finais.

18.24. A solução deverá ser capaz de exportar a chave de criptografia do local de armazenamento das credenciais (cofre), para ser utilizada nos cenários de recuperação de desastres, de forma a conceder acesso à todas as senhas de identidades privilegiadas gerenciadas pela solução.

18.25. A solução não deverá permitir a abertura do cofre com chaves criptográficas geradas por seus respectivos fornecedores e/ou fabricantes em hipótese alguma.

18.26. A solução deve suportar integrar-se com soluções de autenticação de duplo fator através de protocolo Radius ou SAML.

18.27. A solução deve disponibilizar a opção de autenticação utilizando certificados (Smart Cards) e protocolo SAML 2.0.

18.28. A solução deve prover uma interface gráfica para que os administradores possam configurar as integrações com dispositivos e/ou plataformas que não são disponibilizadas nativamente, sem a necessidade de serviços profissionais de terceiros.

18.29. A solução deve integrar-se diretamente, sem codificação adicional ou adição de scripts, com soluções de SIEM, a fim de garantir o registro e a visualização, a partir da aplicação existente nesses sistemas, das seguintes ações:

18.29.1. Atividades administrativas relacionada a acesso as credenciais privilegiadas;

18.29.2. Atividades de recuperação, liberação e alterações de senhas;

18.29.3. Outras atividades de executadas pelos usuários na console web.

18.30. A solução deve suportar, sem necessidade de licenciamento adicional, a gestão de senhas no código fonte em aplicações e scripts (AAPM) através de uma API REST,

18.31. A solução deve possuir API REST, onde as aplicações consomem a senha com requisições à interface API REST, assim evitando que as senhas fiquem expostas no código fonte das aplicações,

18.32. A solução deve possuir deve possuir mecanismo de cache para suportar milhares de requisições pelas aplicações simultaneamente.

18.33. A solução deve possuir mecanismo de segurança que libera o acesso a REST API somente a aplicativos autorizados, incluindo, no mínimo, filtro de IP de origem e autenticação por certificados.

18.34. A solução deve descobrir e alterar credenciais Windows, incluindo contas nomeadas, administradores 'built-in' e convidados.

18.35. A solução deve gerenciar credenciais de Banco de Dados, incluindo Microsoft SQL Server, PostgreSQL, Oracle, MongoDB, MySQL.

18.36. A solução deve descobrir e alterar credenciais privilegiadas em ambientes Linux.

18.37. Gerenciar credenciais em interfaces de gerenciamento de servidores "out-of-band", suportando, no mínimo, Dell iDRAC e HP iLO.

18.38. A solução deve descobrir e alterar credenciais do Active Directory (AD) e todos os outros serviços de diretório compatíveis com LDAP, sem necessidade de adaptações ou scripts.

18.39. O Sistema deve ser capaz de realizar a descoberta, armazenamento e gestão de chaves SSH em sistemas Linux.

18.40. A solução deve identificar as contas privilegiadas com ID 0 em Linux e as contas que não possuem ID zero, porém, são privilegiadas através do uso de ´sudo´ (configuradas no Sudoers).

18.41. A solução deve permitir o agrupamento lógico de sistemas a fim de simplificar a configuração de políticas apropriadas para diferentes tipos de sistemas alvo. Além de permitir a atualização de uma mesma conta em múltiplos sistemas-alvo com uma única tarefa de alteração de senhas.

18.42. Ser capaz de redefinir senhas individuais ou grupos de senhas sob demanda e deve ser capaz de realizar verificações agendadas e automáticas a fim de garantir que as senhas das contas gerenciadas pela solução no dispositivo de destino, correspondam às mesmas senhas armazenadas no banco de dados da solução. Caso a senha da conta gerenciada pela solução seja diferente daquela armazenada no banco de dados, a solução deve ser capaz de gerar relatórios e alertas notificando este evento.

18.43. Conceder acesso aos sistemas utilizando "Remote Desktop" e "SSH" sem que os usuários vejam qualquer senha, garantindo que não haja necessidade de instalação de aplicações e/ou agentes nas estações dos usuários para realizar o acesso, devendo conceder acesso a:

18.43.1. Sistemas ou aplicações parametrizáveis, onde a aplicação deverá ser executada, por meio de página web, devidamente autenticada com usuário e senha pré-determinados ou recuperados da base de dados da solução. Não deverá ser necessária interatividade por parte do usuário no processo de login ao sistema operacional do servidor de destino. Deverá ser possível habilitar a gravação da sessão caso seja necessário.

18.43.2. Sistemas baseados em Remote Desktop e SSH sem que os usuários vejam a senha. A senha vigente no momento (estática ou dinâmica) deverá ser provida para as aplicações ou conexões remotas devendo ser recuperadas de forma automática e transparente do banco de dados da solução.

18.44. As sessões acessadas podem ser monitoradas por meio de gravação de vídeos das mesmas, em formato padrão de execução da solução.

18.45. A solução deve permitir que um administrador possa bloquear, desbloquear e terminar uma sessão ativa caso julgue necessário.

18.46. Monitorar comandos executados ao longo da sessão gravada, possibilitando pesquisar ações específicas no vídeo gravado.

18.47. A solução deve possuir a opção de terminar a sessão automaticamente em uma sessão SSH se o usuário digitar um comando não autorizado.

18.48. A solução deve permitir que as sessões SSH e RDP abertas através da solução sejam terminadas de forma automática ao expirar o tempo requisitado de sessão.

18.49. A solução deve permitir que seja forçado o logoff do usuário em sessões RDP terminadas pela solução ao final do tempo de requisição da sessão.

18.50. A solução deve permitir que os usuários solicitem acesso aos gestores através de interface Web, preferencialmente, em HTML5.

18.51. A solução deve fornecer uma aplicação Web para acessar as funcionalidades básicas que seja compatível, no mínimo, com Internet Explorer, Google Chrome e Firefox.

18.52. Oferecer em sua aplicação web diferentes visões de acordo com as permissões dos usuários mostrando, por exemplo, apenas os ativos e contas delegadas àquele usuário.

18.53. A solução deve permitir o envio automático de logs para servidores SYSLOG de forma aderente ao disposto em RFC 5424 - The Syslog Protocol (IETF).

18.54. A solução deve registrar cada acesso incluindo, no mínimo, os acessos via aplicação web para solicitações de senha, aprovações, retirada de senhas, mudanças de delegação e relatórios. Devem ser registrados os acessos à Console de Gerenciamento tanto para configuração quanto para relatórios, bem como todas as atividades de alterações de senhas.

18.55. Criar relatórios que podem ser exportados em formatos editáveis suportando, no mínimo, os formatos HTML e derivados, CSV, XLSX ou XLS.

18.56. A solução deve suportar também a criação de relatórios que podem ser exportados em formatos não-editáveis suportando, no mínimo, o formato PDF.

18.57. O gerenciamento de identidades privilegiadas deverá disponibilizar:

18.57.1. Mecanismo de retirada e devolução de contas e senhas compartilhadas;

18.57.2. Definição de tempo de validade: permitir o estabelecimento de tempo de validade para as senhas de identidades privilegiadas gerenciadas que forem requisitadas;

18.57.3. Troca automática da senha no sistema gerenciado, após a sua devolução;

18.57.4. Troca automática da senha no sistema gerenciado, após o vencimento do tempo de validade estabelecido;

18.57.5. Configuração de calendário de requisição de senhas de identidades privilegiadas com base em usuários ou grupos de usuários;

18.57.6. Troca de Senhas por Demanda: Permitir a troca de senhas nos Sistemas Gerenciados, de forma individual ou por grupos customizáveis, manualmente ou de forma automática, por agendamento (Grupo de Todos os Sistemas Operacionais , por exemplo);

18.58. Dessa forma, no processo de definição da política de composição de senha, a solução deve ser capaz de:

18.58.1. Gerar senhas aleatórias com extensão de 128 (cento e vinte e oito) caracteres ou mais.

18.58.2. Utilizar caracteres alfabéticos (maiúsculos e minúsculos), numéricos e símbolos.

18.58.3. Especificar qual o tipo de caractere na composição das senhas a serem geradas.

18.58.4. Suportar controle de acesso baseado em papéis, garantindo aderência ao princípio dos privilégios mínimos, e viabilizando a segregação de funções entre usuários de uma mesma aplicação gerenciada. Deve permitir a formação de grupos de usuários e dispositivos, bem como a atribuição de privilégios de acesso a esses Grupos, onde esses privilégios de acessos possam ser atribuídos por critérios como tipo de dispositivo: sistemas operacionais, banco de dados.

18.58.5. Permitir a determinação de quais símbolos estão excluídos ou exclusivamente permitidos na composição da senha.

18.58.6. Garantir a configuração de mecanismo para que as senhas randomizadas sejam únicas para cada credencial.

18.58.7. Garantir a configuração de mecanismo para que determinados grupos de senhas randomizadas sejam as mesmas para cada credencial pertencente a este grupo.

18.59. Permitir a definição de fluxos de aprovação (workflows) para obtenção de acesso às contas privilegiadas, com as seguintes características:

18.59.1. Personalização de fluxos: Permitir a configuração de fluxos para aprovação, de acordo com a criticidade e características da conta (como de acesso emergencial, de uso por terceiros), e aprovação de pelo menos um responsável;

18.59.2. Permitir a aprovação perante um agendamento de ações administrativas, ou seja, a aprovação do acesso ocorrera em um dia, mas a liberação da senha ocorrerá de forma automática somente na data e horário previstos;

18.59.3. A solução deve ser capaz, caso seja necessário, de substituir as senhas de identidades privilegiadas que estejam sendo utilizadas por determinado serviço ou tarefas agendadas do Windows em todos os locais onde estejam sendo utilizadas;

18.59.4. Caso seja necessário, após alteração da senha de identidade privilegiada associada à um serviço, a solução deverá ser capaz de reinicializar o mesmo.

18.59.5. A descoberta automática deve ser realizada por buscas no Active Directory (AD) e/ou por ranges de endereços IP.

18.60. Sobre as características da interface Web para acesso de recuperação das senhas, a solução deverá ser capaz de:

18.60.1. Suportar de forma nativa a personalização dinâmica e automática dos acessos atribuídos ao usuário conforme privilégios delegados pelo administrador da solução.

18.60.2. Permitir que as páginas Web sejam personalizadas de acordo as preferências de linguagem individuais do usuário, inclusive com o idioma em Português.

18.61. A solução deve fornecer relatórios de conformidade detalhados das operações realizadas pela solução, tais como:

18.61.1. Lista de sistemas gerenciados;

18.61.2. Senhas armazenadas;

18.61.3. Eventos de alteração de senha;

18.61.4. Auditoria de contas;

18.61.5. Auditoria de sistemas;

18.61.6. Auditoria de usuários;

18.61.7. Detalhes das próximas atualizações de senha programadas;

18.61.8. Sistemas que estão usando uma conta de serviço para iniciar um ou mais serviços.

18.62. A solução deve fornecer relatórios de auditoria que disponibilizem detalhes das interações dos usuários com a solução, tais como:

18.62.1. Auditoria detalhada, com no mínimo, atividade de login e logoff dos usuários;

18.62.2. Alterações nas funções de delegação;

18.62.3. Adições, deleções, alterações de senhas gerenciadas pela solução;

18.62.4. Operações das senhas dos usuários, incluindo check-in e checkout, solicitações negadas e permitidas;

18.62.5. Os relatórios devem ser filtrados por período de tempo, tipo de operação, sistema, gerente e assim por diante.

18.63. O Sistema deve possuir função de monitoramento e análise de comportamento que toma por base os eventos gerados por todos os itens desta especificação técnica.

18.64. Através dos eventos coletados, deve montar perfis de comportamento dos usuários do sistema.

18.65. A solução deve alertar abusos e comportamentos fora dos padrões aprendidos/mapeados.

18.66. A solução deve monitorar e exibir acessos e atividades realizadas no próprio sistema.

18.67. A solução deverá exibir o somatório das atividades diárias divididos por origem.

18.68. A solução deve detectar, pelo menos, os seguintes comportamentos anormais:

18.68.1. Acessos excessivos a contas privilegiadas;

18.68.2. Usuários potencialmente não confiáveis utilizando acessos administrativos ou contas locais;

18.68.3. Primeira liberação de senha para uma conta gerenciada em um sistema;

18.68.4. Usuários não conseguem recuperar a senha para uma solicitação aprovada ou se a senha é recuperada mais de uma vez.

18.69. Deve fornecer meio de integração para que soluções de terceiros possam encerrar sessões suspeitas (ex: SIEM executa terminação de sessão) através de integração via API.

18.70. Deve permitir a configuração de eventos críticos a serem reportados automaticamente, baseados em comandos Linux em sessões SSH, com suporte a expressões regulares para comandos em geral.

18.71. Módulo de Acesso Remoto Seguro:

18.71.1. O Módulo de acesso remoto seguro de executar em appliance virtual on-premises suportando, no mínimo, VMWARE 7.0.

18.71.2. O Módulo de acesso remoto seguro deve suportar o acesso externo a rede, sem necessidade de uma VPN.

18.71.3. A solução deve ser implantada localmente, com modelo de alta disponibilidade, continuidade de negócios e formas de recuperação de desastre;

18.71.4. A solução deve permitir o acesso a vários tipos de Sistemas Operacionais, com ou sem agentes, incluindo, no mínimo, o suporte a estações de trabalho Windows 10, Servidores Windows Server 2012, 2016 e 2019 e Linux RedHat Enterprise 6.x, 7.x e 8.x;

18.71.5. A solução não deve utilizar protocolos de comunicação legados necessários para o acesso, fazendo uso de TLS 1.2 ou superior;

18.71.6. A solução deve suportar seu funcionamento dentro de redes que não estão diretamente conectadas à internet;

18.71.7. A solução deve suportar o acesso desacompanhado, sem necessidade de permissão prévia a desktops e servidores;

18.71.8. A solução deve possibilitar o acesso a dispositivos de rede como roteadores, switches e outros dispositivos via SSH. Este acesso deve ser feito de forma local, sem que haja a necessidade de trafegar estes protocolos em redes inseguras e/ou liberando-os em regras de firewall;

18.71.9. A solução deve disponibilizar ao usuário, no mínimo, as seguintes formas de acesso a console da solução:

18.71.9.1. Console instalada na estação do usuário, suportando os sistemas operacionais Windows em 32 e 64 Bit, MacOs e Linux em 32 ou 64Bit;

18.71.9.2. Console de acesso Web, preferencialmente em HTML5, sem necessidade de nenhum plug-in ou agente especial para fornecer o acesso.

18.71.10. A solução deve oferecer suporte a provedores de identidade externos para autenticação suportando, no mínimo, servidores LDAP, Active Directory, RADIUS ou Kerberos, bem como atribuir privilégios com base na hierarquia e nas configurações de grupo já especificadas nos respectivos servidores.

18.71.11. Suportar integração com soluções de autenticação de dois fatores via RADIUS ou SAML.

18.71.12. A solução deve suportar logon único (SSO), comunicando-se com um provedor de identidade usando SAML 2.0.

18.71.13. A solução deve suportar o uso de um certificado válido assinado por uma CA.

18.71.14. A solução deve possuir políticas para controlar quando os ativos podem ser acessados suportando, no mínimo:

18.71.14.1. Programação para definir quando os ativos sob esta política podem ser acessados. A política deve permitir a definição do fuso horário a ser utilizado no agendamento, permitindo uma ou mais opções de agendamento do acesso. Definindo o dia e hora de início e o dia e hora de término;

18.71.14.2. Para certos grupos de usuários, a solução deve permitir forçar o encerramento da sessão. Forçando a sessão a se desconectar no horário final agendado. Nesse caso, o usuário deve receber notificações antes de ser desconectado;

18.71.14.3. Notificar destinatários quando uma sessão é iniciada. Suportando, no mínimo, uma notificação por e-mail a destinatários designados sempre que uma sessão é iniciada com qualquer ativo;

18.71.14.4. Notificar destinatários quando uma sessão é terminada. Suportando, no mínimo, uma notificação por e-mail a destinatários designados sempre que uma sessão é encerrada com qualquer ativo;

18.71.15. A solução deve manter uma gravação completa e à prova de falsificação de todas as atividades da área de trabalho e do shell de comandos.

18.71.16. A solução deve manter um registro completo de todas as atividades executadas durante a sessão executada pelos usuários.

18.71.17. A solução deve permitir o monitoramento ao vivo das sessões de acesso, e também deve permitir que os administradores encerrem sessões em andamento, se necessário.

18.71.18. A solução deve permitir a configuração de permissões granulares, oferecendo a capacidade de controlar e delegar permissões por usuários e por função.

18.71.19. A solução deve ser capaz de controlar quais aplicativos podem ser usados por um operador na sessão, limitando o acesso a aplicativos especificados no sistema remoto, permitindo somente os executáveis listados (whitelist) ou negando apenas os executáveis listados (blacklist). Deve ser possível também optar por permitir ou negar o acesso à área de trabalho.

18.71.20. A solução deve suportar filtro de comandos durante as sessões SSH, visando evitar que o usuário, inadvertidamente, use um comando que pode causar danos ao servidor acessado.

18.71.21. A solução deve suportar a injeção automática de credenciais, permitindo que os usuários autentiquem ou elevem privilégios para desktops e sistemas remotos, sem revelar credenciais e senhas de texto simples. Deverá ser permitido ao usuário selecionar a credencial a ser utilizada a partir de uma lista de credenciais que têm privilégios nos sistemas aprovados para acesso.

18.71.22. A injeção de senhas deve suportar a integração com a solução de gerenciamento de acessos privilegiados, permitindo que seus usuários usem as senhas armazenadas na solução.

18.71.23. Ao acessar um ativo baseado em Windows, a injeção de credenciais deve ser suportada na tela de login, bem como a ação especial "Executar como".

18.71.24. Ao acessar um ativo baseado em Linux, injeção de credenciais deve suportar sua utilização em conjunto com o SUDO.

18.71.25. A solução deve suportar o acesso a desktops, servidores e outros sistemas remotos autônomos, suportando os seguintes modos:

18.71.25.1. Através de clientes instalados, que permite o acesso a qualquer sistema Windows, Mac ou Linux. Tendo total gerência e relatórios centralizados de todos os clientes implantados;

18.71.25.2. Acesso através de cliente de proxy local, que permite o acesso a sistemas Windows autônomos em uma rede, sem cliente pré-instalado;

18.71.25.3. Acesso via cliente de proxy para acessar sistemas em uma rede remota que não tenha uma conexão de internet nativa.

18.71.26. Integração com RDP (Remote Desktop Protocol) da Microsoft para realizar sessões utilizando protocolo RDP. Permitindo que os usuários colaborem em sessões e estas sessões possam ser auditadas e gravadas automaticamente.

18.71.27. Acesso a dispositivos de rede habilitados para SSH através de um cliente de proxy efetuando a conexão localmente;

18.71.28. Acesso a servidores VNC onde os usuários podem colaborar em sessões e ter as sessões auditadas e gravadas automaticamente;

18.71.29. Acesso a páginas Web a partir de agente de proxy local, onde os usuários receberão apenas uma conexão a uma página Web local em uma sessão auditada e gravada;

18.71.30. Túnel de protocolos que permitem estender os recursos de conectividade e auditoria remotas de aplicativos proprietários e/ou de terceiros, como sistemas de controle de integração ou ferramentas de banco de dados personalizadas sem necessidade de VPN;

18.71.31. A solução deve permitir o monitoramento em tempo real das sessões de acesso feitas a ativos publicados na ferramenta;

18.71.32. A solução deve permitir que os administradores possam encerrar as sessões em andamento, se necessário;

18.71.33. A solução deve permitir configuração de tempos limites de sessão ociosos, onde seja possível definir o tempo máximo para que um usuário inativo seja desconectado automaticamente;

18.71.34. A solução deve permitir que os usuários transfiram arquivos da máquina em que está conectado para o sistema remoto, através da console da solução e sem necessidade de uso de ferramentas de terceiros;

18.71.35. A solução deve permitir que os usuários compartilhem sessões de acesso com outros usuários do sistema, permitindo que os administradores colaborem em uma mesma sessão. Esta colaboração deve ser possível com usuários internos e também com usuários externos através de convite;

18.71.36. Em caso de colaboração de administradores em uma mesma sessão, a solução deve oferecer chat entre usuários através da mesma console da conexão;

18.71.37. A solução deve oferecer aos usuários conectados a capacidade de ver informações do sistema sem que seja necessário ter acesso a console do ativo;

18.71.38. A solução deve oferecer aos usuários a capacidade de executar tarefas do sistema fora do compartilhamento de tela, com por exemplo reiniciar um serviço em servidores com sistema operacional Windows;

18.71.39. A solução deve oferecer a opção de prover acesso à linha de comandos dos servidores sem a necessidade de compartilhamento de tela, permitindo aos administradores a execução de comandos remotos via conexões lentas de internet;

18.71.40. A solução deve oferecer uma opção de guardar os scripts comuns utilizados pelos administradores como uma opção na console de acesso, permitindo que os administradores executem estes scripts através de um menu de opções;

18.71.41. A solução deve permitir que os usuários reiniciem um sistema durante a sessão e reconectem-se automaticamente quando ativo estiver on-line novamente;

18.71.42. A solução deve permitir que os usuários acessem e editem o registro do Windows de forma remota, sem precisar do compartilhamento de tela;

18.71.43. A solução deve permitir o uso de credenciais armazenadas na solução de gerenciamento de acesso privilegiado para executar ações especiais, permitindo a execução de aplicativos (função de "executar como");

18.71.44. A solução deve permitir que o Administrador mude o portal externo com a marca corporativa, isto é, os administradores podem alterar a imagem de logotipo para exibição em páginas da Web voltadas para o público. Permitindo que os usuários externos verifiquem que estão no site de sua organização, além de aprimorar o portal de acesso com a marca da organização;

18.71.45. Solução deve possuir relatórios das sessões de acesso, onde seja possível visualizar todas as sessões, e detalhes destas sessões que incluem informações básicas da sessão, detalhes da sessão, transcrições de bate-papo e gravações em vídeo de compartilhamento de tela, shells de comando e utilização de túnel de protocolos;

18.71.46. A solução deve possuir relatórios da sessão detalhados que possuam um registro da transcrição completa do bate-papo, o número de arquivos transferidos e ações específicas que ocorreram durante a sessão. Devem contar também com eventos do Windows que apresentam alterações visuais óbvias em uma sessão, incluindo principalmente alterações nas janelas em primeiro plano, contendo o nome do executável e o título da janela;

18.71.47. A solução deve conter informações da sessão que incluem a duração da sessão, endereços IP locais e remotos e informações do sistema remoto.

18.71.48. A solução deve apresentar em relatório as sessões que possuem a gravação ativada, uma opção para reprodução de vídeo de sessões individuais, incluindo legendas de quem estava no controle do mouse e do teclado em qualquer ponto determinado durante a sessão.

18.71.49. Caso o usuário utilize a opção de túnel de sessão, deve ser possível visualizar as gravações de vídeo da área de trabalho inteira do usuário.

18.71.50. Caso o usuário utilize somente o prompt de comando do sistema, deve ser possível visualizar gravações e/ou transcrições de texto de todos os comandos executados durante a sessão.

18.71.51. A solução deve também conter relatórios resumidos que fornecem uma visão geral da atividade ao longo do tempo por usuário. Contendo informações como: O número total de sessões executadas, o número médio de sessões por dia da semana e a duração média das sessões.

18.71.52. A solução deve possuir relatórios de atividades das equipes, que devem conter informações sobre os usuários conforme eles entram ou saem do console de acesso da ferramenta, assim como mensagens de bate-papo enviadas entre membros da equipe, ações de compartilhamento de tela de usuário para usuário e arquivos compartilhados e baixados.

19. ITEM 2 - SERVIÇO DE INSTALAÇÃO, CONFIGURAÇÃO E TRANSFERÊNCIA DE CONHECIMENTO

19.1. A Contratada será inteiramente responsável pela instalação da solução, bem como pelas despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

19.2. A instalação da solução deverá ser realizada presencialmente no ambiente Tribunal Superior Eleitoral e, remotamente, no ambiente dos Tribunais Regionais Eleitoral;

19.3. A instalação da solução deverá ser realizada em dias úteis, podendo ocorrer no período de 10h às 19hs, considerando o fuso horário do contratante;

19.4. O processo de instalação da solução deverá ser acompanhado por servidores do Contratante;

19.5. Para garantir que a instalação não afetará o ambiente do Contratante, os procedimentos e atividades deverão ser realizados por técnicos certificados na solução;

19.6. A Contratada deverá se reunir com a equipe técnica do Contratante e elaborar um plano de instalação, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço;

19.7. A contratada deverá realizar a instalação de todos os módulos adquiridos, bem como realizar a configuração do gerenciamento de acesso privilegiado em 10 (dez) dispositivos, sendo eles 3 (três) servidores linux, 2 (dois) servidores de domínio Windows, 1 (um) VMWARE Vcenter, 2 (dois) Hosts ESXi e 2 (dois) equipamentos de firewall.

19.7.1. No caso do Tribunal Superior Eleitoral, deverá ser configurado ainda o acesso aos 4 (quatro) balanceadores de carga e aos 2 (dois) storage Isilon.

19.7.2. Caso o Tribunal Regional Eleitoral possua necessidade distinta do especificado no item 19.7, esta poderá ser negociada com a Contratada, desde que mantido o quantitativo de 10 (dez) equipamentos.

19.8. A instalação da solução no ambiente do Contratante não poderá interferir no bom funcionamento de outros sistemas previamente instalados;

19.9. A transferência de conhecimento deverá ser realizada no próximo dia útil após a conclusão do serviço de instalação e configuração da solução;

19.10. O repasse de conhecimento deverá ter duração mínima de 20 (vinte) horas;

19.11. A Contratada deverá realizar a transferência de conhecimento para a equipe técnica do Contratante, por meio de repasse de conhecimento nas tecnologias da solução;

19.12. A transferência de conhecimento deverá ser realizada de forma remota, por meio de ferramenta a ser acordada com o Contratante;

19.13. A transferência de conhecimento deverá conter conteúdo teórico e prático sobre a solução e deverá abordar, no mínimo, os seguintes itens:

19.13.1. Detalhamento dos componentes da solução, suas interconexões e todas as informações técnicas necessárias para o seu pleno funcionamento.

19.13.2. Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes da solução, informando as interconexões realizadas com a infraestrutura existente no Contratante.

19.13.3. Orientar sobre os componentes, procedimentos de instalação e administração da solução, explorando as funcionalidades disponíveis na solução ofertada, ainda que não exigidas na especificação técnica.

19.14. A transferência de conhecimento deverá ser realizada por técnicos qualificados e certificados pelo fabricante dos softwares da solução ofertada.

19.15. Concluir instalação, configuração e transferência de conhecimento da solução no prazo de 30 (trinta) corridos, contados do recebimento provisório.

19.16. Caso seja de comum acordo entre o Contratante e a Contratada, as atividades remotas relacionadas no item 19 e subitens poderão ser realizadas presencialmente.

ANEXO I-II - MODELO DE PROPOSTA

Razão Social:		E-mail:	CNPJ:
Endereço:	Cidade:	CEP:	Tel.:

Tabela - Licitação por Lote

Lote	Item	Descrição*	Unidade de Medida	Quantidade	Valor Unitário (R$)	Valor Total (R$)
ÚNICO	1	Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses.	Licenças	14.267		
	2	Serviço de instalação, configuração e transferência de conhecimento.	Serviço	26		
					Valor Total do Lote (R$)	

* A licitante deverá apresentar as características técnicas dos componentes da solução ofertada no lote, indicando marca/modelo dos componentes ofertados.

1. Os documentos técnicos deverão ser apresentados junto com a proposta, por planilha, contendo o item, a descrição do item, e a comprovação técnica de atendimento.
2. As especificações das características técnicas da solução de segurança ofertada deverão estar descritas de forma clara e detalhada.

Declarações:
i) Esta empresa declara que tem pleno conhecimento das condições necessárias para a prestação dos serviços.
ii) Esta empresa declara que nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto desta Licitação.
iii) Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos.

Validade da Proposta:
O prazo de validade desta proposta é de (<*não inferior a 60 dias*>) dias, contados da data de abertura do Pregão.

Local e data.

_____
Nome do Responsável Legal
Cargo/Função

ANEXO I-III - LISTAS DE VERIFICAÇÃO

TERMO DE RECEBIMENTO PROVISÓRIO				
Processo SEI Relacionado: **Contratada:** **CNPJ nº:** **Contrato TSE nº:** **Objeto:** **Vigência:**				
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**				
LISTA DE VERIFICAÇÃO				
ITEM	**ANÁLISE DOS ASPECTOS DE EXECUÇÃO E ENTREGA:**	**SIM**	**NÃO**	**N.A.**
1	**PARA O ITEM 1:**			
1.1	As licenças entregues correspondem ao objeto contratado?			
1.2	As licenças foram entregues no prazo estipulado?			
2	**PARA O ITEM 2:**			
2.1	Os serviços de instalação foram realizados dentro do prazo previsto?			
2.2	Os serviços de instalação foram realizados nas quantidades previstas no contrato?			
2.3	A transferência de conhecimento foi realizada?			
RELATÓRIO DE OCORRÊNCIAS				
RECEBIMENTO PROVISÓRIO DO OBJETO				
Diante da entrega dos serviços pela Contratada e observada a posterior avaliação detalhada dos aspectos quantitativos e qualitativos a ser efetuada durante o Recebimento Definitivo, essa fiscalização decide por:				
	RECEBER PROVISORIAMENTE O OBJETO, **RESSALVADAS EVENTUAIS OCORRÊNCIAS DESCRITAS NESTE DOCUMENTO.**			
	NÃO RECEBER PROVISORIAMENTE O OBJETO.			

TERMO DE RECEBIMENTO DEFINITIVO				
Processo SEI Relacionado: **Edital de Licitação TSE nº:** **Contratada:** **CNPJ nº:** **Contrato nº:** **Objeto:** **Vigência:**				
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**				
ITEM	**CRITÉRIO DE CONFERÊNCIA**	**SIM**	**NÃO**	**N.A**
1	**ASPECTOS QUANTITATIVOS:**			
1.1	A quantidade de licenças é igual à definida no contrato?			
1.2	As licenças entregues possuem as funcionalidades exigidas em contrato?			
1.3	Os serviços de instalação foram realizados nas quantidades previstas no contrato?			
2	**ASPECTOS QUALITATIVOS**:			
2.1	A Solução possui especificações compatíveis com o Edital e correspondentes à proposta da licitante vencedora?			
2.2	Todas as licenças estão registradas em nome do contratante, com o prazo de garantia técnica e atualizações pelo período de 60 meses?			
3	**OUTRAS OBRIGAÇÕES CONTRATUAIS**:			
3.1	Em caso de reprovação de itens, os problemas foram sanados em no máximo 5 (cinco) dias úteis após a notificação?			
3.2	A Contratada realizou a instalação e configuração dentro do prazo contratado?			
	HOUVE ABERTURA DE PROCESSO ADMINISTRATIVO PARA APLICAÇÃO DE PENALIDADES? **SEI nº:**			
RELATÓRIO DE OCORRÊNCIAS				
RECEBIMENTO DEFINITIVO DO OBJETO				
Efetuada a análise de conformidade do objeto com as especificações do Contrato e do Termo de Referência, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide por:				
	RECEBER DEFINITIVAMENTE O OBJETO			
	NÃO RECEBER DEFINITIVAMENTE O OBJETO			

ANEXO I-IV - QUANTIDADE MÍNIMA

Tabela - Licitação por Lote				
Lote	**Item**	**Descrição***	**Unidade de Medida**	**Quantidade**
ÚNICO	1	Solução de Gerenciamento de Acessos Privilegiados, com garantia técnica de 60 (sessenta) meses.	Licenças	150
	2	Serviço de instalação, configuração e transferência de conhecimento.	Serviço	1

ANEXO I-V - TERMO DE CONFIDENCIALIDADE

Eu, _____, inscrito(a) sob RG n.º _____ e CPF n.º _____, colaborador da empresa _____, estabelecida no endereço _____, inscrita no CNPJ com o n.º _____, em razão da execução das atividades previstas do Contrato TSE nº _____, tomei conhecimento de informações sobre o ambiente computacional do Tribunal Superior Eleitoral – TSE e aceito as regras, condições e obrigações constantes no presente Termo.

1. O objetivo deste Termo de Confidencialidade e Sigilo é prover a necessária e adequada proteção às informações restritas de propriedade exclusiva do Tribunal Superior Eleitoral - TSE.
2. A expressão "informação restrita" abrangerá toda informação escrita, oral ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a técnicas, projetos, especificações, desenhos, cópias, diagramas, fórmulas, modelos, amostras, fluxogramas, croquis, fotografias, plantas, programas de computador, discos, disquetes, fitas, contratos, planos de negócios, processos, projetos, conceitos de produto, especificações, amostras de ideia, clientes, nomes de revendedores e/ou distribuidores, preços e custos, definições e informações mercadológicas, invenções e ideias, outras informações técnicas, financeiras ou comerciais, dentre outros.
3. Neste ato comprometo a não reproduzir e/ou dar conhecimento a terceiros, sem a anuência formal e expressa do TSE, das informações restritas reveladas.
4. Estou ciente que as informações reveladas fiquem limitadas ao conhecimento dos diretores, consultores, prestadores de serviços, empregados e/ou prepostos que estejam diretamente envolvidos nas discussões, análises, reuniões e demais atividades relativas à prestação de serviços ao TSE, devendo cientificá-los da existência deste Termo e da natureza confidencial das informações restritas reveladas.
5. Obrigo-me, perante o TSE, informar imediatamente qualquer violação das regras de sigilo estabelecidas neste Termo que tenha ocorrido por sua ação ou omissão, independentemente da existência de dolo.
6. O presente Termo tem natureza irrevogável e irretratável, permanecendo em vigor desde a data da assinatura de contrato entre o Tribunal Superior Eleitoral – TSE e a _____.

E, por aceitar todas as condições e as obrigações constantes no presente Termo, assino-o.

Brasília, ____ de _____ de 20____.

Assinatura: _____

ANEXO I-VI - DESIGNAÇÃO DE PREPOSTO

DESIGNAÇÃO DE PREPOSTO

A empresa **Nome da Empresa**, com sede na **Endereço da empresa**, na cidade de **Cidade**, (**UF**), CNPJ nº **000.000.000/0000-0**, neste ato representada pelo seu **Cargo do Representante**, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Representante**, em atenção ao art. 44 da IN MPDG nº 5/2017, DESIGNA, o(a) Senhor(a) **Nome do Colaborador**, portador(a) da Carteira de Identidade nº **Identidade do Colaborado**, CPF nº **CPF do Colaborador**, para atuar como preposto no âmbito do **Contrato TSE nº xx/xxxx.**

2. O preposto designado representará a empresa perante o Tribunal Superior Eleitoral, zelará pela boa execução do objeto contratual, exercendo os seguintes poderes e deveres:

a)	Participar da reunião inaugural a ser agendada com a fiscalização do contrato.
b)	Ser acessível ao Contratante, por intermédio de número de telefones fixos e celulares que serão informados no momento da indicação.
c)	Comparecer, sempre que solicitado pelo fiscal do contrato, no prazo máximo de 24 (vinte e quatro) horas, para exame e esclarecimentos de quaisquer ocorrências, salvo em situações emergenciais de pronto atendimento.
d)	Agilizar os contatos com os representantes da administração durante a execução do contrato.
e)	Desenvolver outras atividades de responsabilidade da Contratada, principalmente quanto ao controle de informações relativas ao seu contrato e apresentação de documentos quando solicitado.

3. A comunicação entre o preposto e o Tribunal Superior Eleitoral será efetuada por meio dos telefones fixo **(DDD) 00000-0000** e celular **(DDD) 00000-0000** ou do e-mail **email@email.com.br.**

4. A **Nome da Empresa** compromete-se a manter atualizados, durante toda fase de execução da contratação, os contatos de telefone e e-mail para comunicação com o Tribunal Superior Eleitoral.

Anexo I-VII - Quantitativos do TSE e TRE

TRIBUNAL	ITEM 1	ITEM 2
TRE - AC	194	1
TRE - AL	476	1
TRE - AM	280	1
TRE - AP	238	1
TRE - BA	249	1
TRE - CE	870	1
TRE - DF	673	1
TRE - ES	350	1
TRE - GO	601	1
TRE - MA	385	1
TRE - MG	982	1
TRE - MS	-	-
TRE - MT	503	1
TRE - PA	422	1
TRE - PB	400	1
TRE - PE	313	1
TRE - PI	420	1
TRE - PR	600	1
TRE - RJ	669	1
TRE - RN	465	1
TRE - RO	460	1
TRE - RR	312	1
TRE - RS	-	-
TRE - SC	570	1
TRE - SE	493	1
TRE - SP	442	1
TRE - TO	400	1
TSE	2500	1
TOTAL REGISTRADO	14.267	26

TRIBUNAL REGIONAL ELEITORAL DO ACRE	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	40
Servidores: hipervisor VMWARE, VMs, Windows e Linux	116
Instâncias de banco de dados Oracle, MS SQL	8
Instâncias de aplicações/serviços corporativos/senhas hardcode	30
Total	194

TRIBUNAL REGIONAL ELEITORAL DE ALAGOAS	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	190
Servidores: hipervisor VMWARE, VMs, Windows e Linux	151
Instâncias de banco de dados Oracle, MS SQL	35
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	476

TRIBUNAL REGIONAL ELEITORAL DO AMAZONAS	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	20
Servidores: hipervisor VMWARE, VMs, Windows e Linux	200
Instâncias de banco de dados Oracle, MS SQL	10
Instâncias de aplicações/serviços corporativos/senhas hardcode	50
Total	280

TRIBUNAL REGIONAL ELEITORAL DO AMAPÁ	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	120
Servidores: hipervisor VMWARE, VMs, Windows e Linux	98
Instâncias de banco de dados Oracle, MS SQL	3
Instâncias de aplicações/serviços corporativos/senhas hardcode	17
Total	238

TRIBUNAL REGIONAL ELEITORAL DA BAHIA	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	40
Servidores: hipervisor VMWARE, VMs, Windows e Linux	171
Instâncias de banco de dados Oracle, MS SQL	8
Instâncias de aplicações/serviços corporativos/senhas hardcode	30
Total	249

TRIBUNAL REGIONAL ELEITORAL DO CEARÁ	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	350
Servidores: hipervisor VMWARE, VMs, Windows e Linux	475
Instâncias de banco de dados Oracle, MS SQL	5
Instâncias de aplicações/serviços corporativos/senhas hardcode	40
Total	870

TRIBUNAL REGIONAL ELEITORAL DO DISTRITO FEDERAL	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	380
Servidores: hipervisor VMWARE, VMs, Windows e Linux	160
Instâncias de banco de dados Oracle, MS SQL	3
Instâncias de aplicações/serviços corporativos/senhas hardcode	130
Total	673

TRIBUNAL REGIONAL ELEITORAL DO ESPÍRITO SANTO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	50
Servidores: hipervisor VMWARE, VMs, Windows e Linux	180
Instâncias de banco de dados Oracle, MS SQL	20
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	350

TRIBUNAL REGIONAL ELEITORAL DO GOIÁS	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	246
Servidores: hipervisor VMWARE, VMs, Windows e Linux	238
Instâncias de banco de dados Oracle, MS SQL	27
Instâncias de aplicações/serviços corporativos/senhas hardcode	90
Total	601

TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	120
Servidores: hipervisor VMWARE, VMs, Windows e Linux	160
Instâncias de banco de dados Oracle, MS SQL	5
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	385

TRIBUNAL REGIONAL ELEITORAL DE MINAS GERAIS	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	390
Servidores: hipervisor VMWARE, VMs, Windows e Linux	315
Instâncias de banco de dados Oracle, MS SQL	33
Instâncias de aplicações/serviços corporativos/senhas hardcode	244
Total	982

TRIBUNAL REGIONAL ELEITORAL DO MATO GROSSO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	167
Servidores: hipervisor VMWARE, VMs, Windows e Linux	168
Instâncias de banco de dados Oracle, MS SQL	18
Instâncias de aplicações/serviços corporativos/senhas hardcode	150
Total	503

TRIBUNAL REGIONAL ELEITORAL DO PARÁ	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	120
Servidores: hipervisor VMWARE, VMs, Windows e Linux	260
Instâncias de banco de dados Oracle, MS SQL	7
Instâncias de aplicações/serviços corporativos/senhas hardcode	35
Total	422

TRIBUNAL REGIONAL ELEITORAL DA PARAÍBA	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	96
Servidores: hipervisor VMWARE, VMs, Windows e Linux	163
Instâncias de banco de dados Oracle, MS SQL	21
Instâncias de aplicações/serviços corporativos/senhas hardcode	120
Total	400

TRIBUNAL REGIONAL ELEITORAL DE PERNAMBUCO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	54
Servidores: hipervisor VMWARE, VMs, Windows e Linux	172
Instâncias de banco de dados Oracle, MS SQL	7
Instâncias de aplicações/serviços corporativos/senhas hardcode	80
Total	313

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	120
Servidores: hipervisor VMWARE, VMs, Windows e Linux	220
Instâncias de banco de dados Oracle, MS SQL	10
Instâncias de aplicações/serviços corporativos/senhas hardcode	70
Total	420

TRIBUNAL REGIONAL ELEITORAL DO PARANÁ	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	235
Servidores: hipervisor VMWARE, VMs, Windows e Linux	350
Instâncias de banco de dados Oracle, MS SQL	5
Instâncias de aplicações/serviços corporativos/senhas hardcode	10
Total	600

TRIBUNAL REGIONAL ELEITORAL DO RIO DE JANEIRO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	435
Servidores: hipervisor VMWARE, VMs, Windows e Linux	166
Instâncias de banco de dados Oracle, MS SQL	15
Instâncias de aplicações/serviços corporativos/senhas hardcode	53
Total	669

TRIBUNAL REGIONAL ELEITORAL DO RIO GRANDE DO NORTE	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	200
Servidores: hipervisor VMWARE, VMs, Windows e Linux	190
Instâncias de banco de dados Oracle, MS SQL	20
Instâncias de aplicações/serviços corporativos/senhas hardcode	55
Total	465

TRIBUNAL REGIONAL ELEITORAL DE RONDÔNIA	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	100
Servidores: hipervisor VMWARE, VMs, Windows e Linux	250
Instâncias de banco de dados Oracle, MS SQL	10
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	460

TRIBUNAL REGIONAL ELEITORAL DE RORAIMA	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	80
Servidores: hipervisor VMWARE, VMs, Windows e Linux	124
Instâncias de banco de dados Oracle, MS SQL	8
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	312

TRIBUNAL REGIONAL ELEITORAL DE SANTA CATARINA	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	200
Servidores: hipervisor VMWARE, VMs, Windows e Linux	250
Instâncias de banco de dados Oracle, MS SQL	20
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	570

TRIBUNAL REGIONAL ELEITORAL DE SERGIPE	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	195
Servidores: hipervisor VMWARE, VMs, Windows e Linux	178
Instâncias de banco de dados Oracle, MS SQL	20
Instâncias de aplicações/serviços corporativos/senhas hardcode	100
Total	493

TRIBUNAL REGIONAL ELEITORAL DE SÃO PAULO	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	34
Servidores: hipervisor VMWARE, VMs, Windows e Linux	342
Instâncias de banco de dados Oracle, MS SQL	11
Instâncias de aplicações/serviços corporativos/senhas hardcode	55
Total	442

TRIBUNAL REGIONAL ELEITORAL DO TOCANTINS	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	30
Servidores: hipervisor VMWARE, VMs, Windows e Linux	280
Instâncias de banco de dados Oracle, MS SQL	10
Instâncias de aplicações/serviços corporativos/senhas hardcode	80
Total	400

TRIBUNAL SUPERIOR ELEITORAL	
Ativo	Quantidade
Dispositivos de rede: LAN, WAN, WI-FI, Firewalls, IPS, Balanceadores de Carga, Antispam	200
Servidores: hipervisor VMWARE, VMs, Windows e Linux	1700
Instâncias de banco de dados Oracle, MS SQL	100
Instâncias de aplicações/serviços corporativos/senhas hardcode	500
Total	2500

ADAÍRES AGUIAR LIMA
SECRETÁRIO(A) DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **01/12/2021, às 19:20**, 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=1863670&crc=A1746F22, informando, caso não preenchido, o código verificador **1863670** e o código CRC **A1746F22.**