TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

Contrato Nº 17/2022

CONTRATO TRE-PI Nº 17/2022

CONTRATO DE FORNECIMENTO/PRESTAÇÃO DE SERVIÇOS QUE ENTRE SI CELEBRAM O TRIBUNAL REGIONAL DO PIAUÍ E A EMPRESA DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.

O TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, CNPJ 05.957.363/0001-33, situado à Praça Des. Edgar Nogueira, S/N – Centro Cívico, bairro Cabral, em Teresina – PI, neste ato representado por seu Vice-Presidente, no exercício da Presidência, Desembargador JOSÉ JAMES GOMES PEREIRA, na sequência designado simplesmente **CONTRATANTE** e, de outro lado, a empresa **DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA**, CNPJ 09.650.283/0001-91, com sede no SCN Quadra 02, Bloco D, Torre A, nº 810 - Liberty Mall - Brasíliia/DF, CEP. 70.712-903, Telefones (61) 3030-1000 / 9.9291-7070, daqui por diante denominada CONTRATADA, neste ato representada por seu diretor executivo FABRÍCIO BOMBARDA GUEDES, email fabricio@dfti.com.br, têm justo e acordado celebrar o presente **CONTRATO DE FORNECIMENTO/PRESTAÇÃO DE SERVIÇOS**, sob a regência das Leis nº 8.666/93 e nº 10.520/2002, decorrente da Licitação TSE nº 84/2021, modalidade pregão, na forma eletrônica e da Ata de Registro de Preços TSE nº 01/2022, constantes do Procedimento Administrativo SEI nº 2021.00.000003531-9 TSE, mediante as seguintes cláusulas e condições:

CLÁUSULA PRIMEIRA - DO OBJETO

O presente contrato tem por objeto a **contratação de Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses,** conforme especificações, exigências e prazos constantes do Anexo I do Edital da Licitação TSE nº 84/2021, modalidade pregão, na forma eletrônica (item 3 da ARP TSE 01/2022) e proposta da CONTRATADA, que passam a fazer parte deste instrumento, independentemente de transcrição, no que não conflitar com as disposições do edital e deste instrumento.

CLÁUSULA SEGUNDA - DA EXECUÇÃO

A execução do objeto do presente contrato, na forma descrita em sua Cláusula Primeira, será realizada por meio do estabelecimento da CONTRATADA, inscrito no CNPJ nº 09.650.283/0001-91, de acordo com o Edital da Licitação, seu Anexo I e proposta vencedora.

CLÁUSULA TERCEIRA - DAS OBRIGAÇÕES DO CONTRATANTE

O CONTRATANTE:

1 - Prestará as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA.

2 - Acompanhará, fiscalizará e atestará a execução contratual, bem como indicará as ocorrências verificadas.

3 - Designará servidor ou comissão de servidores para fiscalizar a execução do objeto contratual.

3.1- 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.

4- Permitirá que os funcionários da CONTRATADA, desde que devidamente identificados, tenham acesso aos locais de execução do objeto.

5- Recusará qualquer produto/serviço entregue em desacordo com as especificações constantes do Termo de Referência - Anexo I do Edital da Licitação ou com defeito.

5.1- Ao Tribunal Superior Eleitoral fica reservado o direito de recusar de pronto a solução que flagrantemente não esteja em conformidade com a especificação do Termo de Referência - Anexo I do Edital da Licitação.

6 - Receber a CONTRATADA para reunião inaugural, conforme prazo definido no item 10.1 do Termo de Referência - Anexo I do Edital da Licitação (Cronograma de Execução).

7- Realizará o recebimento dos produtos/serviços conforme detalhado no Capítulo 11 do Termo de Referência - Anexo I do Edital da Licitação.

8 - Efetuará o pagamento à CONTRATADA segundo as condições estabelecidas na Cláusula Sexta deste contrato.

CLÁUSULA QUARTA - DAS OBRIGAÇÕES DA CONTRATADA

A CONTRATADA obriga-se a:

1 - Executar, com observação dos prazos e exigências, todas as obrigações e especificações técnicas constantes do Termo de Referência - Anexo I do Edital da Licitação.

1.1 - A CONTRATADA deverá cumprir os eventos descritos no Cronograma de Execução constante da tabela prevista no item 10.1 do Termo de Referência- Anexo I do Edital da Licitação, respeitando os prazos máximos estabelecidos, os quais poderão ser antecipados sempre que as circunstâncias assim o permitam.

2 - Assinar o termo de confidencialidade disponível no Anexo I-V do Termo de Referência - Anexo I do Edital da Licitação.

3 - Entregar as subscrições no prazo máximo de 30 (trinta) dias corridos, contados do início da vigência do contrato. As licenças deverão ser entregues em formato digital, para o e-mail *nscib@tre-pi.jus.br*, ou para download em site do fabricante do produto.

3.1 - As licenças deverão possuir data de validade a partir do recebimento definitivo efetuado pelo CONTRATANTE.

3.1.1. A validade usual de mercado deve ser comprovada, sendo de, no mínimo, 72 (setenta e dois) meses, contados da data de fabricação, não podendo ter transcorrido mais de 30 (trinta) dias do prazo de validade no momento da entrega.

3.2 - O endereço da sede do TRE-PI fica situado na Praça Des. Edgar Nogueira, S/N – Centro Cívico, bairro Cabral, em Teresina – PI, CEP 64.000-920, de segunda a sexta-feira, das 07h00 às 13h00 . Telefone do Núcleo de Segurança Cibernética-NSCIB (86) 2107-9816.

3.3 - Caso a solução necessite de banco de dados específico e proprietário para funcionamento da solução, as licenças deste deverão ser fornecidas pela CONTRATADA junto com a solução ofertada sem ônus para o CONTRATANTE, além daquele já cotado em sua proposta.

3.4 - As licenças de sistema operacional e do ambiente de virtualização, bem como o equipamento para execução da solução serão fornecidos pelo CONTRATANTE.

3.5 - A CONTRATADA será responsável por qualquer ônus decorrente de marcas, registros e patentes relativos ao fornecimento.

4 - Instalar, configurar e ativar as subscrições conforme especificações e prazos estabelecidos no Termo de Referência - Anexo I do Edital da Licitação.

5 - Providenciar a renovação das subscrições nos 30 (trinta) dias que antecederem o vencimento das mesmas, com validade a partir do vencimento das subscrições ativas.

5.1 - As subscrições renovadas devem ser entregues e ativadas, no máximo, até o vencimento das subscrições em uso de modo a não haver interrupção nos serviços.

5.2 - Cabe à CONTRATADA ativar as subscrições na ferramenta instalada.

6 - Prestar o serviço de suporte técnico durante todo o período de validade das subscrições e conforme as condições e exigências estabelecidas no Capítulo 8 do Termo de Referência - Anexo I do Edital da Licitação.

6.1 - O suporte técnico deve ser prestado durante todo o período de validade das subscrições.

6.2 - Os serviços de suporte pertinentes ao **item contratado** deverão ser realizados por técnicos do fabricante ou por técnicos da CONTRATADA, certificados na solução.

6.3 - Observar os prazos de resposta para problemas ocorridos durante o período de suporte. Tais prazos estão previstos na tabela contida no item 9.5 do Termo de Referência - Anexo I do Edital da Licitação e são contados do recebimento da notificação de abertura do chamado.

7 - Responsabilizar-se pelas despesas decorrentes do fornecimento dos produtos e da execução dos serviços objeto do Termo de Referência - Anexo I do Edital da Licitação.

8 - Manter, durante toda a vigência do contrato, os dados atualizados do preposto, na forma do Anexo I-IV do Edital da Licitação.

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

8.2 - 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.

8.3 - 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.

9 - Refazer ou corrigir os serviços não aprovados pela fiscalização e cumprir as obrigações pendentes em até 5 (cinco) dias corridos, contados da notificação do CONTRATANTE.

10 - Acatar as recomendações efetuadas pelo fiscal do contrato.

11 - Responsabilizar-se pelos danos causados diretamente à Administração ou a terceiros, decorrentes de culpa ou dolo na execução do objeto do Termo de Referência - Anexo I do Edital da Licitação.

12 - 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.

13 - 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).

14 - 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.

15 - 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 TSE.

16 - Manter, durante a execução do contrato as condições de habilitação exigidas na licitação.

16.1 - Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a CONTRATADA terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.

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

17.1 - A inadimplência da CONTRATADA com referência aos encargos suportados não transfere a responsabilidade por seu pagamento ao contratante, nem poderá onerar o objeto deste contrato.

18 - Observar durante a execução do contrato os critérios de sustentabilidade previstos no item 19.3 do Termo de Referência - Anexo I do Edital da Licitação.

19 - Manter, durante toda a vigência da contratação, o constante do item 8 do Capítulo VI do Edital da Licitação, caso o critério tenha sido utilizado como desempate na licitação.

20 - Não transferir a outrem, no todo ou em parte, a parcela de maior relevância do objeto deste contrato. Todavia, fica permitida a subcontratação do próprio fabricante para execução dos serviços de suporte técnico.

20.1 - A subcontratação só será autorizada pelo CONTRATANTE após a comprovação da capacidade técnica da empresa para executar os serviços pretendidos e de sua regularidade fiscal.

CLÁUSULA QUINTA - DO PREÇO CONTRATUAL E DO REAJUSTE

1 - O preço a ser pago à CONTRATADA pelo fornecimento/prestação dos serviços objeto deste contrato, são os constantes em sua proposta, atualizada com o último preço ofertado e aceito no pregão, sendo de **R$ 46.000,00 (quarenta e seis mil reais)** o valor total deste contrato (para o período de 60 meses).

LOTE	ITEM	DESCRIÇÃO	QTD	VALOR UNITARIO	VALOR ANUAL DO CONTRATO	VALOR TOTAL DO CONTRATO (60 MESES)
1	3	contratação de 200 (duzentas) subscrições de solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox (Item 03 da ARP 01/2020 TSE), com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	200	R$ 46,00	R$ 9.200,00	R$ 46.000,00

2 - Os preços a serem pagos à CONTRATADA pelas licenças serão fixos e irreajustáveis pelo período de 12 (doze) meses iniciais. Após esse período, o reajuste será feito de ofício, podendo ocorrer negociação entre as partes, momento no qual, será apreciada a possibilidade da aplicação do índice IPCA-IBGE, no período entre o mês básico da apresentação da proposta e o mês anterior ao reajuste, compreendendo sempre o período de 12 meses, de acordo com a seguinte fórmula:

PR = IMR x PA/IMM

Onde:

PR = Preço reajustado

IMR = Índice do IPCA-IBGE do mês anterior ao reajuste

IMM = Índice do IPCA-IBGE do mês de apresentação da proposta

PA = Preço anteriormente praticado

3 - A administração antes de conceder o reajuste poderá exigir que a CONTRATADA apresente planilha demonstrativa com a efetiva variação de seus custos ocorrida no período

do reajuste proposto.

CLÁUSULA SEXTA - DA LIQUIDAÇÃO E DO PAGAMENTO

1 - O pagamento do objeto do presente contrato será efetuado após o recebimento definitivo dos produtos/serviços nos termos estabelecidos no Capítulo 12 do Termo de Referência - Anexo I do Edital de Licitação TSE nº 84/2021, até o 10º (décimo) dia útil a partir da atestação da 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.

1.1 - O pagamento ocorrerá anualmente, sendo o mesmo procedimento para as subscrições e para as suas renovações anuais.

1.1.1 - A CONTRATADA deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento no ato da entrega do objeto e quando das renovações anuais das subscrições.

1.2 - O atesto do objeto contratado se dará pelo fiscal, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA. O fiscal terá o prazo de até 2 (dois) dias úteis para emitir a NTA e remeter o processo a 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.

2 - Na fase de liquidação e pagamento da despesa deverá ser verificada pela área competente a regularidade fiscal da CONTRATADA perante a Seguridade Social, Fazenda Federal (Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União fornecida pela Receita Federal do Brasil), o Fundo de Garantia do Tempo de Serviço - FGTS, e, ainda, perante a Justiça do Trabalho (Certidão Negativa de Débito Trabalhista – CNDT); admitida a certidão positiva com efeito de negativa ou outra equivalente na forma da lei.

3 - O CNPJ constante da nota fiscal/fatura deverá ser o mesmo indicado na proposta e na nota de empenho.

4 - Nos casos de pagamento efetuados após 30 (trinta) dias da emissão do Termo de Recebimento Definitivo ou da apresentação da nota fiscal, conforme o caso, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo TSE, entre o 31º (trigésimo primeiro) dia e a data da emissão da ordem bancária, será a seguinte:

EM = I x N x VP
Onde:
EM = encargos moratórios;
N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;
VP = valor da parcela a ser paga;
I = 0,0001644 **{**(índice de compensação financeira por dia de atraso, assim apurado I = (6/100)/365)**}**.

CLÁUSULA SÉTIMA - DOS CRÉDITOS ORÇAMENTÁRIOS

A despesa decorrente do fornecimento/prestação dos serviços objeto do presente contrato correrá à conta dos créditos orçamentários consignados no Orçamento da União à Justiça Eleitoral, para o Exercício de 2022, Natureza de Despesa 339040 - Serviços de Tecnologia da Informação e Comunicação – Pessoa Jurídica, na Ação 02.122.0033.20GP.0022 – Julgamento de Causas e Gestão Administrativa.

CLÁUSULA OITAVA - DAS SANÇÕES ADMINISTRATIVAS

1 - Nos termos do artigo 7º da Lei nº 10.520/2002, caso a CONTRATADA descumpra total ou parcialmente o objeto contratado, garantida a prévia defesa e o contraditório, ficará sujeita às seguintes penalidades:
1.1 - advertência;
1.2 - multa;
1.3 - impedimento de licitar e contratar com a União e descredenciamento no SICAF, pelo prazo de até 5 (cinco) anos.
2 - Será aplicada a penalidade descrita no subitem 1.3, à CONTRATADA que:
2.1 - apresentar documentação falsa;
2.2 - causar o atraso na execução do objeto do contrato;
2.3 - falhar ou fraudar na execução do contrato;
2.3.1 - para efeito de aplicação do disposto no subitem 2.3 desta Cláusula, será considerada falha na execução do contrato os casos de inexecução total, e os de inexecução parcial que resultem na rescisão contratual;
2.4 - comportar-se de modo inidôneo;
2.5 - declarar informações falsas; ou
2.6. cometer fraude fiscal.
3 - Com fundamento no art. 7º da Lei nº 10.520/2002, as sanções previstas nos subitens 1.1 e 1.3, poderão ser aplicadas à CONTRATADA juntamente com as multas convencionais e de mora, podendo estas serem descontadas dos pagamentos a serem efetuados, após o encerramento do procedimento de apuração de penalidades, e quando cabível, sem prejuízo do ressarcimento dos danos causados à Administração e das demais cominações legais.
3.1 - Para efeito de aplicação das penas de advertência e multa, às infrações são atribuídos graus, conforme as tabelas seguintes:

-

TABELA DE CORRESPONDÊNCIA	
GRAU	**PERCENTUAL**

-

1	Advertência
2	0,5% sobre o valor total da parcela não cumprida
3	1% sobre o valor total da parcela não cumprida
4	2% sobre o valor total da parcela não cumprida
5	5% sobre o valor total da parcela não cumprida
6	10% sobre o valor total do contrato

TABELA DE INFRAÇÃO					
ITEM	**DESCRIÇÃO**	**INCIDÊNCIA**	**LIMITE MÁXIMO DE APLICAÇÃO DE MORA**	**GRAU**	**ULTRAPASSADO O LIMITE MÁXIMO DE APLICAÇÃO**
1	Deixar de cumprir quaisquer das obrigações previstas no Edital de Licitação TSE n° 84/2021 e seus anexos e não elencadas nesta tabela de multas	Por ocorrência	1 (uma) ocorrência por obrigação	1	Vide item 2 desta Tabela.
2	Reincidir no descumprimento da mesma obrigação punida com advertência.	Por ocorrência	3 (três) ocorrências	2	Será configurada a inexecução parcial do contrato com aplicação de multa de 5% do valor total da parcela não cumprida
3	Deixar de cumprir o prazo para entrega do objeto.	Por dia corrido	10 (dez) dias corridos	3	Será configurada a inexecução total do contrato com aplicação de multa de 10% do valor da parcela não cumprida no caso da não entrega total do objeto; ou Inexecução parcial do contrato com aplicação de multa de 15% do valor da parcela não cumprida no caso de entrega parcelada já aceita pelo contratante.
4	Deixar de cumprir o prazo para substituição do objeto/correção dos serviços recusados durante o recebimento.	Por dia corrido	10 (dez) dias corridos	4	Será configurada a inexecução parcial do contrato com aplicação de multa de 15% do valor da parcela não cumprida.
5	Deixar de cumprir os prazos para o primeiro atendimento dos chamados durante a vigência da garantia técnica.	Por hora	6(seis)horas	2	Será configurada a inexecução parcial do contrato com aplicação de multa de 5% do valor da parcela não cumprida.
6	Deixar de cumprir os prazos para a implementação da solução técnica definitiva ou solução de contorno durante a vigência da garantia técnica.	Por hora	6(seis)horas	4	Será configurada a inexecução parcial do contrato com aplicação de multa de 15% do valor da parcela não cumprida.
7	Suspender ou interromper, salvo motivo de força maior ou caso fortuito, os serviços contratuais.	Por hora	6(seis)horas	5	Será configurada a inexecução parcial do contrato com aplicação de multa de 20% do valor da parcela não cumprida.
8	Manter empregado sem qualificação para executar os serviços contratados.	Por ocorrência	2(duas) ocorrências	5	Será configurada a inexecução parcial do contrato com aplicação de multa 20% do valor da parcela não cumprida.
	Permitir situação que cause ou crie perigo de dano físico ou lesão corporal.	Por ocorrência	1(uma) ocorrência	6	Será configurada a inexecução total do contrato com aplicação de multa de 10% sobre o valor total do contrato

10	Permitir situação que cause consequências letais.	Por ocorrência	1 (uma) ocorrência	6	Será configurada a inexecução total do contrato com aplicação de multa de 10% sobre o valor total do contrato
11	Deixar de atingir o percentual de 70% de aprovação da transferência de conhecimento.	Por ocorrência	2(duas) ocorrências	5	Será configurada a inexecução parcial do contrato com aplicação de multa 20% do valor total da parcela não cumprida.

4 - Ultrapassado o limite máximo de aplicação de mora previsto na tabela de infração, a Administração poderá optar uma das seguintes hipóteses:

4.1 - Rescindir o contrato com aplicação das sanções previstas na coluna "ultrapassado o limite máximo de aplicação" da tabela de infração, sem prejuízo das demais consequências previstas em lei e neste contrato.

4.2 - Presente o interesse público, aceitar o objeto mediante justificativa, com aplicação apenas da multa de mora.

4.3 - Entregue apenas parte do objeto, não aceitar o restante e rescindir o contrato, com aplicação das sanções previstas na coluna “ultrapassado o limite máximo de aplicação”, sem prejuízo das demais consequências previstas em lei e neste contrato.

4.3.1 - A aceitação de parte do objeto só será possível mediante demonstração nos autos de que sua recusa causará prejuízo à Administração.

4.4 - A multa de mora não será cumulada com a multa proveniente de uma inexecução total ou parcial. As multas de mora que já tiverem sido quitadas terão seu valor abatido do montante apurado da multa por inexecução total ou parcial, considerando-se para esse fim cada lote como um contrato em apartado.

5 - Na apuração das penalidades previstas nesta Cláusula, a autoridade competente poderá considerar, além das previsões legais, contratuais e dos Princípios da Administração Pública, as seguintes circunstâncias:

5.1 - a natureza e a gravidade da infração contratual;

5.2 - o dano que o cometimento da infração ocasionar à Administração;

5.3 - a vantagem auferida em virtude da infração;

5.4 - as circunstâncias gerais agravantes e atenuantes;

5.5 - os antecedentes da CONTRATADA.

6 - Os prazos de adimplemento das obrigações contratadas admitem prorrogação nos casos e condições especificados no § 1º do art. 57 da Lei nº 8.666/1993, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito com antecedência mínima de 3 (três) dias úteis do seu vencimento, anexando-se documento comprobatório do alegado pela CONTRATADA, ficando a aceitação da justificativa a critério do CONTRATANTE.

6.1 - O prazo mínimo de antecedência acima pode ser reduzido para as situações imprevisíveis que impeçam o cumprimento da obrigação no prazo ajustado.

7 - Se a CONTRATADA não recolher o valor da multa que lhe for aplicada, dentro de 5 (cinco) dias úteis a contar da data da intimação para o pagamento, a importância será descontada automaticamente, ou ajuizada a dívida, consoante o art. 86 da Lei nº 8.666/93, acrescida de juros moratórios de 0,5% (meio por cento) ao mês.

8 - O CONTRATANTE promoverá o registro no SICAF de toda e qualquer penalidade imposta à CONTRATADA.

9 - O período de atraso será contado em dias corridos, salvo disposição em contrário.

10 - Fica estabelecido que os casos omissos serão resolvidos entre as partes contratantes, respeitados o objeto do presente contrato, a legislação e demais normas reguladoras da matéria, em especial as Leis nº 8.666/93 e nº 10.520/2002, aplicando-lhe, quando for o caso, supletivamente, os princípios da Teoria Geral dos Contratos e as disposições do Direito Privado.

11 - Os atos administrativos de aplicação das sanções, com exceção de advertência, multa de mora e convencional, serão publicados resumidamente no Diário Oficial da União.

CLÁUSULA NONA - DOS RECURSOS ADMINISTRATIVOS

Dos atos administrativos concernentes ao presente contrato cabe recurso nos termos do art. 109 da Lei nº 8.666/1993.

CLÁUSULA DEZ - DA RESCISÃO

O CONTRATANTE poderá rescindir o presente contrato, sem prejuízo das penalidades contratuais ou legais, no caso de sua inexecução total ou parcial ou nos demais previstos no art. 78 da Lei nº 8.666/1993 e, ainda, pelo descumprimento das condições de habilitação e qualificação legalmente exigidas, assim como das condições constantes deste instrumento e da proposta.

CLÁUSULA ONZE - DAS ALTERAÇÕES

O presente contrato poderá ser alterado na ocorrência de qualquer das hipóteses previstas no art. 65 da Lei nº 8.666/1993.

CLÁUSULA DOZE - DA VIGÊNCIA E DA DURAÇÃO

O presente contrato terá vigência a partir **da publicação do extrato do contrato no DOU** e duração de até 60 (sessenta) meses.

CLÁUSULA TREZE - DO FORO

O foro da Seção Judiciária de Teresina-PI é o competente para solucionar qualquer questão relativa ao presente contrato.

CLÁUSULA QUATORZE - DA PUBLICIDADE

O extrato do presente contrato será publicado no Diário Oficial da União, conforme o disposto no art. 61, parágrafo único, da Lei nº 8.666/1993, correndo as despesas por conta do CONTRATANTE.

E por estarem assim, justas e acordadas, as partes assinam eletronicamente o presente instrumento para todos os fins de direito.

TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ
Desembargador JOSÉ JAMES GOMES PEREIRA
Vice-Presidente, no exercício da Presidência

DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA
FABRICIO BOMBARDA GUEDES
Representante legal

Documento assinado eletronicamente por **Fabricio Bombarda Guedes**, **Usuário Externo**, em 14/07/2022, às 11:48, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **José James Gomes Pereira**, **Presidente, em exercício**, em 18/07/2022, às 10:10, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

TRIBUNAL SUPERIOR ELEITORAL

SECRETARIA DE ADMINISTRAÇÃO

EDITAL DE LICITAÇÃO TSE Nº 84/2021

MODALIDADE: PREGÃO

FORMA: ELETRÔNICA

SISTEMA DE REGISTRO DE PREÇOS

PROCESSO Nº 2021.00.000003531-9

O Tribunal Superior Eleitoral, sediado no Setor de Administração Federal Sul, SAFS Q. 7, Lotes 1 e 2, Brasília/DF, torna público que realizará licitação na modalidade pregão, na forma eletrônica, em atendimento à solicitação da Seção de Suporte a Aplicações, para registro de preços para eventual contratação de subscrições de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento, conforme as especificações, condições, quantidades e prazos constantes do Termo de Referência – Anexo I deste Edital. A licitação será regida pelas Leis nº 8.666/1993 e nº 10.520/2002, pela Lei Complementar nº 123/2006 e pelos Decretos nº 7.892/2013, nº 8.538/2015 e nº 10.024/2019.

A proposta de preços, bem como os documentos de habilitação deverão ser enviados, exclusivamente, por meio do sistema eletrônico, no período compreendido entre as 08 horas do dia 1º de dezembro de 2021 e as 14 horas do dia 10 de dezembro de 2021 (horário de Brasília).

A sessão pública será aberta no dia 15 de dezembro de 2021, às 14 horas, ou no mesmo horário do primeiro dia útil subsequente, na hipótese de não haver expediente na data marcada.

Farão parte deste Registro de Preços, como órgãos participantes, os Tribunais Regionais Eleitorais – TREs, que serão responsáveis pelas suas respectivas contratações.

CAPÍTULO I – DO OBJETO

1. A presente licitação, por **lote único**, tem por objeto o registro de preços para eventual contratação de subscrições de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento, com pagamento anual, pelo período de 60 (sessenta), consoante especificações, condições, quantidades e prazos constantes do Termo de Referência – Anexo I deste Edital.

2. Fazem parte do presente edital os anexos abaixo relacionados:

- Anexo I - Termo de Referência
- Anexo I-I - Especificações Técnicas
- Anexo I-II - Modelo de Proposta
- Anexo I-III - Listas de Verificação
- Anexo I-IV - Designação de Preposto
- Anexo I-V - Termo de Confidencialidade
- Anexo I-VI - Quantidade Mínima
- Anexo I-VII - Quantidade Estimada pelos TREs e TSE
- Anexo II - Minuta de Ata de Registro de Preços
- Anexo II-I - Itens Registrados
- Anexo III - Minuta de Contrato

CAPÍTULO II – DAS CONDIÇÕES PARA PARTICIPAÇÃO

1. Para participar deste pregão eletrônico a licitante deverá preencher os seguintes requisitos:

1.1. Ser credenciada no órgão central do Sistema de Serviços Gerais - SISG, por intermédio do sítio www.comprasgovernamentais.gov.br, que atuará como órgão provedor do Sistema Eletrônico de Compras do Governo Federal.

1.2. Enviar em campo próprio do sistema eletrônico as seguintes declarações virtuais:

- de que cumpre plenamente os requisitos de habilitação e que sua proposta está em conformidade com as exigências do instrumento convocatório;
- de que não emprega menores de 18 anos em trabalho noturno, perigoso ou insalubre nem menores de 16 anos em qualquer trabalho, salvo na condição de aprendiz a partir de 14 anos (Lei nº 9.854/99);
- de quaisquer fatos supervenientes à inscrição cadastral impeditivos de sua habilitação;
- de elaboração independente de proposta; e
- de que atende aos requisitos do art. 3° da LC n.° 123/2006, para fazer jus aos benefícios previstos na referida lei.

1.2.1. A declaração falsa relativa ao cumprimento de qualquer condição sujeitará a licitante às sanções previstas em lei e neste Edital.

1.3. Todos os custos decorrentes da elaboração e apresentação das propostas serão de responsabilidade exclusiva da licitante, não se responsabilizando o Tribunal Superior Eleitoral por quaisquer custos, transações efetuadas pela licitante ou eventual desconexão do sistema.

2. Não poderão participar deste pregão eletrônico:

2.1. Consórcio de empresas;

2.2. Empresas em processo de recuperação judicial, sem plano de recuperação acolhido judicialmente ou certidão emitida pela instância judicial competente ou documento judicial compatível; em processo de recuperação extrajudicial; cuja falência tenha sido decretada; que se encontrem sob concurso de credores; e em dissolução ou em liquidação;

2.3. Empresas que estejam declaradas inidôneas ou impedidas para licitar ou contratar com a Administração Pública Federal, desde que o ato tenha sido publicado no Diário Oficial da União pelo órgão que o praticou, bem como as que tenham sido punidas com suspensão temporária de participação em licitação e impedimento de contratar com o Tribunal Superior Eleitoral;

2.3.1. Será efetuada, pelo Pregoeiro, consulta aos cadastros oficiais: Cadastro Nacional de Condenados por Ato de Improbidade Administrativa e por Ato que implique em Inelegibilidade – CNCIAI, Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS) e Cadastro de Inidôneos do TCU;

2.4. . Empresas que possuam inscrição no cadastro de empregadores flagrados explorando trabalhadores em condições análogas às de escravo, instituído pela Portaria Interministerial MTPS/MMIRDH nº 4/2016;

2.4.1. Será efetuada, pelo Pregoeiro, consulta do nome da empresa na "lista suja" de empregadores flagrados explorando trabalhadores em condições análogas às de escravo emitida pelo Ministério de Trabalho e Previdência, atualizada periodicamente em seu sítio eletrônico (https://www.gov.br/trabalho/pt-br/assuntos/fiscalizacao/combate-ao-trabalho-escravo);

2.5. Empresas ou seus dirigentes que possuam condenação por infringir as leis de combate à discriminação de raça ou gênero, ao trabalho infantil e ao trabalho escravo, em afronta ao que está previsto no art. 1º e no art. 170 da Constituição Federal de 1988; no art. 149 do Código Penal Brasileiro; no Decreto nº 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;

2.5.1. A comprovação será feita mediante Certidão Judicial de Distribuição, informalmente conhecida como "nada consta" ou "certidão negativa", da Justiça Federal e da Justiça Comum, para a licitante e para seus dirigentes, que deverá ser encaminhada juntamente com a proposta e documentos de habilitação na forma definida no item 1 do Capítulo IV deste Edital;

2.5.1.1. Eventual ausência de juntada da Certidão Judicial de Distribuição poderá ser saneada pelo Pregoeiro, por diligência, que solicitará a sua anexação no Sistema *Comprasnet*, na forma do item 3 do Capítulo VIII ou, se necessário, prorrogará o prazo, mediante solicitação justificada da licitante e decisão fundamentada do Pregoeiro, registradas em ata.

CAPÍTULO III – DO CREDENCIAMENTO

1. A licitante deverá credenciar-se no sistema de Compras do Governo Federal, disponível no endereço eletrônico www.comprasgovernamentais.gov.br, no prazo mínimo de 3 (três) dias úteis antes da data de realização do pregão eletrônico.

1.1. O credenciamento é o nível básico do registro cadastral no SICAF que permite a participação dos interessados em qualquer pregão na forma eletrônica e será feito pela atribuição de chave de identificação e de senha pessoal e intransferível para acesso ao sistema eletrônico.

1.2. O credenciamento da licitante, assim como a sua manutenção, dependerá de registro cadastral prévio e atualizado no Sistema de Cadastramento Unificado de Fornecedores – SICAF.

1.3. O credenciamento junto ao provedor do sistema implica a responsabilidade legal da licitante ou de seu representante legal e a presunção de sua capacidade técnica para realização das transações inerentes ao pregão eletrônico.

2. O uso da senha de acesso ao sistema eletrônico é de inteira e exclusiva responsabilidade da licitante, incluindo qualquer transação efetuada diretamente ou por seu representante, não cabendo ao provedor do sistema ou ao Tribunal Superior Eleitoral, promotor da licitação, responsabilidade por eventuais danos decorrentes do uso indevido da senha, ainda que por terceiros.

CAPÍTULO IV – DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

1. A proposta de preços, **com todas as exigências descritas no Capítulo VIII**, bem como os documentos de habilitação exigidos no Capítulo IX deste edital, observado o disposto no item 3 do Capítulo VII deste Edital, deverão ser enviados em formulários específicos, mediante o uso da chave de acesso e senha privativa da licitante, exclusivamente, por meio do sistema eletrônico, no período compreendido no preâmbulo deste Edital.

1.1. A comprovação dos documentos de habilitação que constem do SICAF poderá ser feita, pelo Pregoeiro, mediante consulta on-line ao sistema, assegurando o direito de acesso aos dados às demais licitantes.

1.2. Nesta etapa do certame, não haverá ordem de classificação das propostas, o que ocorrerá somente após os procedimentos de julgamento da proposta.

1.3. Os documentos que compõem a proposta e a habilitação da licitante melhor classificada somente serão disponibilizados para avaliação do Pregoeiro e para acesso público após o encerramento da fase de lances.

1.4. Como condição de participação, as licitantes deverão obrigatoriamente apresentar cotação de preços para todos os itens que compõem o lote.

2. As licitantes se responsabilizarão pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas, assim como os lances inseridos, bem como pelo acompanhamento de todas as operações efetuadas no sistema eletrônico durante a sessão pública, arcando com quaisquer ônus decorrentes da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

3. Até a abertura da sessão, as licitantes poderão retirar ou substituir suas propostas e os documentos de habilitação anteriormente apresentados.

4. A proposta deverá obedecer rigorosamente aos termos deste Edital e seus anexos, não sendo aceita oferta de produtos/serviços com características e quantidades diferentes das indicadas no Termo de Referência – Anexo I deste Edital.

5. O envio da proposta implicará plena aceitação, por parte da licitante, das condições estabelecidas neste Edital e seus Anexos.

6. Os preços oferecidos serão fixos e irreajustáveis, ressalvando-se o disposto nos artigos 17, 18 e 19 do Decreto nº 7.892/2013.

CAPÍTULO V – DA ABERTURA DA SESSÃO

1. No horário previsto no Edital, a sessão pública na internet será aberta por comando do Pregoeiro com a utilização de sua chave de acesso e senha.

2. O Pregoeiro verificará as propostas apresentadas e desclassificará, de forma fundamentada e registrada no sistema, aquelas que estejam em desconformidade com os requisitos estabelecidos neste Edital e seus Anexos.

2.1. A desclassificação de um único item do lote implicará na desclassificação da proposta para todo o lote.

3. O sistema ordenará automaticamente as propostas classificadas pelo Pregoeiro, visto que somente estas participarão da fase de lance.

CAPÍTULO VI – DA COMPETITIVIDADE – FORMULAÇÃO DE LANCES

1. Aberta a etapa competitiva, sessão pública, as licitantes deverão encaminhar lances exclusivamente por meio do sistema eletrônico, sendo a licitante imediatamente informada, *on-line*, do seu recebimento e do valor consignado no registro.

1.1. Os lances serão ofertados pelo valor unitário de cada item que compõe o lote.

1.1.1. Para os itens 1, 2 e 3, o valor unitário corresponde a 60(sessenta) meses.

1.2. As licitantes poderão oferecer lances sucessivos, observados o horário fixado para a abertura da sessão pública e as regras estabelecidas neste Edital.

1.3. A licitante somente poderá oferecer lance inferior ao último por ela ofertado e registrado pelo sistema eletrônico, porém, o lance poderá ser intermediário, ou seja, igual ou superior à melhor oferta registrada.

1.4. Será adotado para o envio de lances neste pregão eletrônico o modo de disputa "**aberto e fechado**", em que as licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.

1.5. A etapa de lances da sessão pública terá duração inicial de 15 minutos. Encerrado esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, que transcorrerá pelo período de até 10 minutos, findo o qual será automaticamente encerrada a recepção de lances.

1.6. Encerrado o prazo previsto no subitem 1.5 deste Capítulo, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até 5 minutos, o qual será sigiloso até o encerramento deste prazo.

1.6.1. Não havendo pelo menos 3 (três) ofertas nas condições definidas no item 1.6, os autores dos melhores lances, na ordem de classificação, até o máximo de 3 (três), poderão oferecer um lance final e fechado em até 5 minutos, o qual será sigiloso até o encerramento deste prazo.

1.7. Após o término dos prazos estabelecidos nos subitens 1.6 e 1.6.1, o sistema ordenará os lances segundo a ordem crescente de valores.

1.7.1. Não havendo lance final e fechado classificado na forma estabelecida nos subitens 1.6 e 1.6.1, haverá o reinício da etapa fechada, para que os demais licitantes, até o máximo de 3 (três), na ordem de classificação, possam ofertar um lance final e fechado em até 5 minutos, o qual será sigiloso até o encerramento deste prazo, observado, após essa etapa, o disposto no subitem 1.7.

1.8. Caso nenhuma licitante classificada na etapa de lance fechado atenda às exigências de habilitação, o Pregoeiro poderá, auxiliado pela equipe de apoio, justificadamente, admitir o reinício da etapa fechada de lance, nos termos dispostos no subitem 1.6.1.

1.9. Se houver mais de um lance de igual valor, prevalecerá aquele registrado em primeiro lugar.

2. As licitantes serão informadas, em tempo real, do valor do menor lance registrado, durante a sessão pública do pregão eletrônico, sendo vedada a identificação do seu detentor.

3. Após a fase de lances, o sistema identificará em coluna própria as microempresas (ME) e empresas de pequeno porte (EPP) participantes, fazendo a comparação entre os valores da primeira colocada, caso esta não seja uma ME ou EPP, e das demais ME ou EPP na ordem de classificação, que será disponibilizada automaticamente nas telas do pregoeiro e do fornecedor e encaminhada mensagem por meio de *chat.*

4. Se o menor lance for ofertado por licitante que não se enquadre na condição de ME ou EPP, o sistema facultará a estas o exercício do direito de preferência para fins de desempate, conforme determina o § 2º do art. 44 da LC nº 123/2006, momento no qual a ME ou EPP mais bem classificada será convocada para apresentar nova proposta, no prazo máximo de 5 (cinco) minutos controlados pelo sistema, sob pena de preclusão, consoante determina o § 3º do art. 45 da LC nº 123/2006.

5. Caso a ME ou EPP convocada decline de exercer o direito de preferência, o sistema convocará as remanescentes que porventura se enquadrem na hipótese do § 2º do art. 44 da LC nº 123/2006, na ordem de classificação.

6. Se houver êxito no procedimento especificado acima, o sistema disponibilizará nova classificação dos fornecedores para fins de aceitação pelo pregoeiro. Não havendo êxito ou não existindo ME ou EPP participante, prevalecerá a classificação inicial.

7. Se houver equivalência de valores apresentados pelas ME ou EPP, que se encontrem no intervalo estabelecido no § 2º do art. 44 da LC nº 123/2006, o sistema efetuará sorteio para identificar a empresa que primeiro poderá apresentar melhor oferta.

8. Havendo equivalência de valores apresentados por empresas em igualdade de condições, será assegurada a ordem de preferência disposta no art. 3º, § 2º da Lei nº 8.666/1993, com redação dada pela Lei nº 12.349 de 15/12/2010.

8.1. No caso de desempate nos termos descritos no item 8 deste Capítulo, a empresa ficará obrigada a cumprir o disposto nesse item durante toda a vigência da contratação, conforme art. 66-A da Lei nº 8.666/1993.

8.2. Na hipótese de persistir o empate, a proposta vencedora será sorteada pelo sistema eletrônico dentre as propostas empatadas.

9. No caso de desconexão do Pregoeiro, no decorrer da etapa competitiva do pregão eletrônico, o sistema poderá permanecer acessível às licitantes para a recepção dos lances, retornando o Pregoeiro, quando possível, sua atuação no certame, sem prejuízo dos atos realizados.

9.1. Quando a desconexão persistir por tempo superior a 10 (dez) minutos, a sessão do pregão eletrônico será suspensa e reiniciada somente após a comunicação expressa aos participantes, com no mínimo, 24 (vinte e quatro) horas de antecedência, no endereço eletrônico www.comprasgovernamentais.gov.br.

CAPÍTULO VII – DA CLASSIFICAÇÃO DAS PROPOSTAS E DO JULGAMENTO DA LICITAÇÃO

1. Encerrada a etapa de lances, o pregoeiro julgará as propostas, adotando o critério de menor preço global do lote e encaminhará contraproposta pelo sistema eletrônico diretamente à licitante que tenha ofertado o melhor preço, para que seja obtida melhor proposta, bem como decidirá sobre sua aceitação, observando-se a adequação ao objeto e a compatibilidade do preço em relação ao estimado para a contratação. A negociação poderá ser acompanhada pelas demais licitantes.

1.1. Embora a classificação final para o lote seja por seu valor total, a disputa será pelo preço unitário de cada item que compõe o lote. A cada lance ofertado (por item), o sistema atualizará automaticamente o valor global do lote, sagrando-se vencedora a licitante que ofertar o menor valor global do lote.

1.1.1. A desclassificação de um único item do lote implicará na desclassificação da proposta para todo o lote.

1.2. Será desclassificada a proposta que apresentar preços manifestamente inexequíveis, assim considerados aqueles que não venham a ter demonstrada sua viabilidade através de documentos que comprovem que os custos dos insumos são coerentes com os de mercado.

1.2.1. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderá ser efetuada diligência, e adotados, entre outros e no que couber, os seguintes procedimentos:

a) questionamentos junto à proponente para a apresentação de justificativas e comprovações em relação aos custos com indícios de inexequibilidade;

b) verificação de acordos, convenções coletivas ou sentenças normativas;

c) levantamento de informações no Ministério do Trabalho e Previdência e consultas às Secretarias de Fazenda Federal, Distrital, Estadual ou Municipal;

d) consultas a entidades ou conselhos de classe, sindicatos ou similares;

e) pesquisas em órgãos públicos ou empresas privadas para verificação de contratos da mesma natureza;

f) pesquisa de preço com fornecedores dos insumos utilizados, tais como atacadistas, lojas de suprimentos, supermercados e fabricantes;

g) verificação de notas fiscais dos produtos adquiridos pelo proponente;

h) levantamento de indicadores salariais ou trabalhistas publicados por órgãos de pesquisa;

i) estudos setoriais;

j) análise de soluções técnicas e/ou condições excepcionalmente favoráveis que o proponente detenha para o fornecimento/prestação dos serviços; e

k) demais verificações que porventura se fizerem necessárias.

2. Aceita a melhor oferta, o Pregoeiro anunciará a licitante classificada em primeiro lugar para o lote, imediatamente depois do encerramento da etapa competitiva da sessão pública ou, quando for o caso, após negociação e decisão acerca do valor, conforme descrito no item 1 deste Capítulo e verificará a habilitação da licitante conforme disposições deste Edital.

3. Os documentos complementares à proposta e à habilitação, quando necessários à confirmação daqueles exigidos no edital e já apresentados, serão solicitados pelo pregoeiro e encaminhados pela licitante melhor classificada, exclusivamente via sistema, após o encerramento do envio de lances, observado o prazo de que trata o item 3 do Capítulo VIII deste Edital.

3.1. O prazo estabelecido poderá ser prorrogado pelo Pregoeiro por solicitação escrita e justificada da licitante, formulada antes de findo o prazo, e formalmente aceita pelo Pregoeiro.

4. Na hipótese de a proposta não ser aceitável ou se a licitante não atender às exigências habilitatórias, o pregoeiro examinará a proposta subsequente até a apuração de uma proposta que atenda aos requisitos descritos neste Edital, em conformidade com o disposto no item 1 deste Capítulo.

5. Constatado o atendimento às exigências fixadas neste Edital, a licitante classificada em primeiro lugar será declarada vencedora da licitação.

6. No julgamento da habilitação e das propostas, o pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas, dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhes validade e eficácia para fins de habilitação e classificação.

6.1. Na hipótese de necessidade de suspensão da sessão pública para a realização de diligências, com vistas ao saneamento de que trata o item 6 deste Capítulo, a sessão pública será reiniciada mediante aviso prévio no sistema com, no mínimo, 24 (vinte e quatro) horas de antecedência, sendo a ocorrência será registrada em ata.

CAPÍTULO VIII –DA PROPOSTA

1. A proposta de preços das licitantes deverá ser elaborada com observância das seguintes exigências:

1.1. não conter cotações alternativas, emendas ou entrelinhas;

1.2. fazer menção ao número deste edital, conter a razão social da licitante, seu CNPJ, dados bancários e endereço completo;

1.2.1. a falta do CNPJ e (ou) endereço completo poderá ser preenchida pelos dados constantes no sistema eletrônico;

1.3. conter cotação de preço unitário e total para todos os itens que compõe o lote, em Real, incluídos todos os tributos, fretes, taxas, suporte técnico, garantia, mão de obra, repasse de conhecimento e demais encargos pertinentes, conforme Modelo de Proposta constante do Anexo I-II do Termo de Referência - Anexo I deste Edital;

1.3.1. embora o critério de julgamento da licitação seja o de menor preço global do lote, a licitante deverá apresentar cotação de preço para todos os itens que compõem o lote;

1.3.2. os preços unitários e totais estimados para os itens são os constantes do Capítulo 15 do Termo de Referência - Anexo I deste Edital;

1.4. vir acompanhada de planilha contendo o item, sua descrição de forma clara e detalhada, bem como a comprovação técnica de atendimento;

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

1.5. conter marca e modelo do produto ofertado;

1.6. indicar o número do CNPJ da filial ou do estabelecimento da licitante que emitirá a nota fiscal referente ao fornecimento/prestação dos serviços, indicação essa indispensável para efeito de empenho da despesa e realização do pagamento nos termos do Capítulo XIII deste Edital.

2. A apresentação da proposta implicará, necessariamente, a anuência a todas as exigências contidas neste Edital e seus Anexos, inclusive quanto aos prazos de execução e condições de garantia constantes do Termo de Referência – Anexo I do Edital, bem como quanto à validade da proposta não inferior a 60 (sessenta) dias, contados da data de sua entrega.

3. Após a fase de lances, a proposta de preços da licitante classificada em primeiro lugar, ajustada ao valor final aceito pelo pregoeiro, juntamente com os documentos de que trata o item 3 do Capítulo VII, quando for o caso, deverá ser anexada ao Sistema Comprasnet após solicitação do Pregoeiro pela opção "**Convocar Anexo**", no prazo de 2 (duas) horas, contado de sua solicitação.

CAPÍTULO IX – DA HABILITAÇÃO DA LICITANTE

1. Para habilitação neste pregão eletrônico, serão exigidos os documentos discriminados abaixo, além da regularidade do cadastramento da licitante perante o Sistema de Cadastramento Unificado de Fornecedores - SICAF, nos níveis I, II, III e VI, conforme art. 6º da IN SEGES/MP nº 3, de 26/04/2018:

1.1. Atestado(s) ou declaração(ões) de capacidade técnica-operacional em nome da empresa, expedido(s) por pessoa(s) jurídica(s) de direito público ou privado, que comprove(m) que a licitante executou a contento entrega de objeto compatível com o descrito no Termo de Referência - Anexo I deste Edital.

1.1.1. Será considerado objeto compatível o fornecimento de licenças de antivírus com prestação de suporte, comprovando-se no mínimo 50 % (cinquenta por cento) do quantitativo total registrado.

1.2. O(s) atestado(s) deverá(ão) conter, no mínimo, as seguintes informações:

1.2.1. O contratante e seu endereço;

1.2.2. Discriminação do serviço prestado;

1.2.3. Volume ou quantidade de serviços realizados;

1.2.4. Período de realização dos serviços;

1.2.5. Manifestação expressa do Contratante de que a licitante "atende(eu) satisfatoriamente ao contrato" ou manifestação do grau de satisfação do cliente (ex.: bom, ótimo, excelente), em relação aos serviços prestados.

1.3. Será admitido o somatório de atestados desde que os serviços tenham sido prestados simultaneamente.

1.4. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior.

2. Para os documentos que têm prazo de validade e este não estiver expresso no documento, será considerada a validade de 90 (noventa) dias, a partir de sua emissão, se outro prazo não estiver fixado em lei.

3. A regularidade do cadastramento das licitantes perante o SICAF, nos níveis exigidos no item 1 deste Capítulo, será verificada mediante consulta *on-line* ao sistema.

3.1. É dever da licitante atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, em conjunto com a apresentação da proposta e documentos, a respectiva documentação atualizada.

3.2. O descumprimento do subitem 3.1 implicará a inabilitação da licitante, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões feita pelo Pregoeiro lograr êxito em encontrar a(s) certidão(ões) válida(s), conforme art. 43, §3º, do Decreto 10.024, de 2019.

3.3. A regularidade no SICAF referente ao nível VI descrito no item 1 deste Capítulo refere-se tanto à Certidão negativa de falência, recuperação judicial ou recuperação extrajudicial, expedida pelo distribuidor da sede da pessoa jurídica quanto ao do balanço patrimonial.

3.4. Caso o balanço patrimonial apresente alguma irregularidade perante o SICAF ou, embora regular, apresente índices de LG, SG, e LC menores que 1, a licitante deverá encaminhá-lo ao Pregoeiro juntamente com as demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira da empresa, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais quando encerrados há mais de 3 meses da data de apresentação da proposta.

3.4.1. Serão considerados na forma da lei o balanço patrimonial e as demonstrações contábeis assim apresentados:

3.4.1.1. publicados em Diário Oficial; ou

3.4.1.2. publicados em jornal de grande circulação; ou

3.4.1.3. por cópia registrada no órgão de registro público competente da sede ou domicílio da licitante; ou

3.4.1.4. por cópia extraída do Livro Diário - devidamente autenticado no órgão de registro público competente da sede ou domicílio da licitante - inclusive com os Termos de Abertura e de Encerramento; ou

3.4.1.5. por cópia extraída do Livro Diário, com o respectivo comprovante de entrega da Escrituração Contábil Digital ao SPED Contábil, juntamente com o termo de autenticação eletrônica realizada pela Junta Comercial; ou

3.4.1.6. outros meios permitidos pelas normas de regência.

3.4.2. A análise da qualificação econômico-financeira será feita por servidores qualificados designados pelo Tribunal Superior Eleitoral e avaliada pelos Índices de Liquidez Geral (LG), Solvência Geral (SG), e Liquidez Corrente (LC), que deverão ser iguais ou superiores a 1 (um):

$$LG = \frac{\text{ATIVO CIRCULANTE + REALIZÁVEL A LONGO PRAZO}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

$$SG = \frac{\text{ATIVO TOTAL}}{\text{PASSIVO CIRCULANTE + PASSIVO NÃO CIRCULANTE}}$$

$$LC = \frac{\text{ATIVO CIRCULANTE}}{\text{PASSIVO CIRCULANTE}}$$

3.4.3. As fórmulas deverão estar devidamente aplicadas em memorial de cálculos juntado ao balanço.

3.4.4. A licitante que apresentar resultado menor do que 1, em quaisquer dos índices - Liquidez Geral - LG, Solvência Geral - SG, e Liquidez Corrente – LC, deverá comprovar Capital Social mínimo ou Patrimônio Líquido mínimo correspondente a 10% do valor total estimado para a contratação, na forma dos §§ 2º e 3º do art. 31 da Lei nº 8.666/93.

3.4.5. Se necessária a atualização do balanço e do patrimônio líquido, deverá ser apresentado, juntamente com esses documentos, o memorial de cálculo correspondente.

3.4.6. As demonstrações contábeis deverão apresentar as assinaturas do titular ou representante da empresa e do contabilista responsável, legalmente habilitado.

3.4.7. As demonstrações contábeis das empresas com menos de um exercício social de existência devem cumprir a exigência contida na lei, mediante a apresentação do Balanço de Abertura ou do último Balanço Patrimonial levantado.

3.4.8. Poderão ser exigidas das empresas, para confrontação com as demonstrações contábeis, as informações prestadas à Receita Federal.

4. Caso a licitante classificada em primeiro lugar esteja enquadrada na condição de ME ou EPP e apresente alguma restrição relativa à regularidade fiscal, será concedido o prazo de 5 (cinco) dias úteis, contados da data da divulgação, por meio do *chat*, do resultado de habilitação do certame, podendo ser concedida a prorrogação por igual período, caso solicitado e mediante a apresentação de justificativa, para regularização da situação, admitindo-se certidões positivas com efeito de negativas, na forma da lei. Findo o prazo, as licitantes serão convocadas para a nova sessão, na qual será registrado, no sistema *Comprasnet*, o resultado de julgamento da habilitação, abrindo-se o prazo para manifestação da intenção de recorrer, conforme descrito no item 1 do Capítulo X deste Edital.

4.1. A não regularização da documentação no prazo previsto implicará a decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 10.520/2002, sendo facultado à Administração convocar as licitantes remanescentes, na ordem de classificação, ou revogar a licitação.

5. As licitantes deverão enviar os documentos exigidos para a habilitação exclusivamente, por meio do sistema eletrônico, conforme disposto no item 1 do Capítulo IV deste Edital.

6. Após a classificação das propostas, havendo a necessidade de envio de documentos complementares à confirmação daqueles exigidos neste edital e já apresentados, os documentos deverão ser apresentados em formato digital, via sistema, no mesmo prazo definido no item 3 do Capítulo VIII deste Edital, por solicitação do Pregoeiro.

6.1. A diligência de que trata o item 6 permite, apenas, a solicitação de documentos outros para confirmação dos já apresentados, sendo exemplo a requisição de cópia de contrato de prestação de serviços que tenha embasado a emissão de atestado de capacidade técnica já apresentado.

7. Atendidas todas as disposições deste Edital, a licitante classificada em primeiro lugar será declarada vencedora, sendo-lhe adjudicado o objeto da licitação, observado o disposto no Capítulo X deste Edital.

CAPÍTULO X – DOS RECURSOS

1. Admitir-se-á, nos termos da legislação vigente, a interposição de recursos, mediante manifestação prévia, imediata e motivada da licitante, feita durante a sessão pública, em campo próprio do sistema, até o prazo final estabelecido pelo Pregoeiro.

2. A apresentação das razões pela recorrente e de eventuais contrarrazões pelas demais licitantes será realizada exclusivamente no âmbito do sistema eletrônico, em formulários próprios, no prazo máximo de 3 (três) dias, contados a partir da data do encerramento da sessão pública e do término do prazo da recorrente, respectivamente, consignado pelo Pregoeiro na respectiva ata, sendo-lhes assegurada vista imediata dos elementos indispensáveis à defesa dos seus interesses.

3. A falta de manifestação imediata e motivada da intenção de interpor recurso, até o prazo final estabelecido pelo Pregoeiro na sessão pública deste pregão eletrônico, implicará a decadência desse direito da licitante, podendo o Pregoeiro adjudicar o objeto à vencedora.

3.1. Apenas na presença dos pressupostos recursais, ou seja, a sucumbência, a tempestividade, a legitimidade, o interesse e a motivação, os recursos serão recebidos (Acórdão TCU n.° 694/2014 – Plenário).

4. Após decididos os recursos e constatada a regularidade dos atos praticados, a autoridade competente do Tribunal Superior Eleitoral adjudicará o objeto e homologará o procedimento licitatório.

5. Os autos do procedimento permanecerão com vista franqueada aos interessados. Para tanto, as empresas interessadas deverão entrar em contato com a secretaria da Comissão Permanente de Licitação, nos dias úteis, pelos telefones 3030-8167/8173, haja vista as medidas de isolamento preventivas à propagação do novo Coronavírus (COVID-19).

CAPÍTULO XI – DA ATA DE REGISTRO DE PREÇOS

1. Após a homologação do resultado do julgamento, a licitante adjudicatária será convocada para firmar a ata de registro de preços, conforme minuta constante no Anexo II deste Edital, no prazo máximo de 5 (cinco) dias úteis, sob pena de decair do direito a ter o seu preço registrado.

2. O prazo fixado no item 1 poderá ser prorrogado uma única vez e por igual período, desde que a solicitação seja apresentada ainda durante o transcurso do interstício inicial, ocorrendo motivo justificado e aceito pelo Tribunal Superior Eleitoral.

3. A ata de registro de preços terá validade de 1 (um) ano, contado da publicação de seu extrato no Diário Oficial da União.

4. É facultado à Administração, quando a licitante convocada não comparecer para assinar a Ata de Registro de Preços no prazo e condições estabelecidos, chamar as licitantes remanescentes, na ordem de classificação, para fazê-lo em igual prazo e nas mesmas condições propostas pela primeira colocada.

4.1. A recusa injustificada da licitante em assinar a ata dentro do prazo estabelecido, ensejará a aplicação das penalidades previstas neste Edital e em lei.

5. Os preços consignados na ata de registro de preços serão fixos e irreajustáveis durante o período de vigência, ressalvando-se o disposto nos arts. 17, 18 e 19 do Decreto n.° 7.892/2013.

CAPÍTULO XII – DA CONTRATAÇÃO

1. Autorizada a contratação, sempre que houver necessidade, será firmado contrato com a empresa adjudicatária, o qual tomará por base os dispositivos da Lei nº 8.666/93, as condições estabelecidas neste Edital e seus anexos, bem como na proposta apresentada pela adjudicatária.

2. Após regular notificação por parte do TSE, a empresa adjudicatária deverá assinar no prazo de 5 (cinco) dias úteis, seguintes à notificação, o termo de contrato (Anexo III), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas no Capítulo XIV deste Edital, obrigando-se em conformidade com as disposições contratuais, do Termo de Referência, da Ata de Registro de Preços e da proposta vencedora.

3. O prazo fixado no item anterior poderá ser prorrogado uma única vez e por igual período, desde que a solicitação respectiva seja apresentada ainda durante o transcurso do interstício inicial, bem como que ocorra motivo justo e aceito pelo TSE.

4. É facultado à Administração, quando a licitante registrada em primeiro lugar não assinar o contrato no prazo e condições estabelecidas, chamar as licitantes remanescentes registradas, obedecida a ordem de classificação, para fazê-lo em igual prazo, podendo, ainda, revogar a licitação, independente da cominação prevista no art. 7º da Lei nº 10.520/2002.

4.1. A recusa injustificada da licitante registrada em assinar o termo de contrato, dentro do prazo estabelecido, ensejará a aplicação das penalidades previstas neste Edital e em lei.

5. A emissão da nota de empenho em favor da contratada só deverá ser efetuada após consulta ao CADIN, conforme estabelece o art. 6º da Lei 10.522/2002.

6. Como condição para celebração do contrato, a licitante adjudicatária deverá informar, nos termos do Anexo I-IV do Termo de Referência - Anexo I deste Edital, nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação como TSE, e ainda, apresentar os seguintes documentos:

6.1. Termo de Confidencialidade, constante do Anexos I-V do Termo de Referência - Anexo I deste Edital, respectivamente, assinado pelo Preposto, em nome da contratada, e por todos os demais funcionários que atuarem na execução da contratação.

6.2. Declaração de que está regularmente inscrita no Regime Especial Unificado de Arrecadação de Tributos e Contribuições devidos pelas ME e EPP - Simples Nacional - para efeito do disposto no inciso XI, art. 4º da IN RFB nº 1234/2012, **se for o caso**, em 2 (duas) vias, assinada pelo seu representante legal, conforme modelo constante do Anexo IV da referida IN.

CAPÍTULO XIII – DA LIQUIDAÇÃO E DO PAGAMENTO

1. O pagamento do objeto da presente licitação será efetuado após o recebimento definitivo dos produtos/serviços nos termos estabelecidos no Capítulo 12 do Termo de Referência - Anexo I deste Edital, até o 10º (décimo) dia útil, a partir da atestação da nota fiscal 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.

1.1. Para os itens 1, 2 e 3 o pagamento ocorrerá anualmente, sendo o mesmo procedimento para as subscrições e para as suas renovações anuais.

1.1.1. A contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento no ato da entrega do objeto e quando das renovações anuais das subscrições.

1.2. Para os item 4 e 5 o pagamento será realizado em parcela única, sendo que:

1.2.1. O pagamento relativo aos serviços descritos no item 4 ocorrerá somente após a conclusão das 28 (vinte e oito) instalações do software de gerência da solução, devendo a contratada entregar o faturamento com toda documentação exigida para liquidação e pagamento após a implantação completa da solução no TSE e demais 27 Tribunais Regionais Eleitorais.

1.2.2. Para o pagamento relativo aos serviços descritos no item 5, a contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento em até 2 (dois) dias úteis após a realização da transferência de conhecimento.

1.3. O atesto do objeto contratado se dará pelo fiscal, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA, conforme previsto na IN nº 11/2021- TSE. O fiscal terá o prazo de até 2 (dois) dias úteis para emitir a NTA e remeter o processo a 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.

1.4. Os Tribunais Regionais Eleitorais participantes deste Registro de Preços se responsabilizarão pelo pagamento à contratada pelo fornecimento dos produtos/prestação dos serviços de acordo com o quantitativo adquirido por cada um deles.

2. Na fase de liquidação e pagamento da despesa deverá ser verificada pela área competente a regularidade fiscal da contratada perante a Seguridade Social, Fazenda Federal (Certidão Conjunta de Débitos relativos a Tributos Federais e à Dívida Ativa da União fornecida pela Receita Federal do Brasil), o Fundo de Garantia do Tempo de Serviço - FGTS, e, ainda, perante a Justiça do Trabalho (Certidão Negativa de Débito Trabalhista – CNDT); admitida a certidão positiva com efeito de negativa ou outra equivalente na forma da lei.

3. O CNPJ constante da nota fiscal/fatura deverá ser o mesmo indicado na proposta e nota de empenho.

4. Nos casos de pagamento efetuados após 30 (trinta) dias da emissão do Termo de Recebimento Definitivo ou da apresentação da nota fiscal, conforme o caso, desde que a contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo TSE, entre o 31º (trigésimo primeiro) dia e a data da emissão da ordem bancária, será a seguinte:

EM = I x N x VP

Onde

EM = encargos moratórios;

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = valor da parcela a ser paga;

I = 0,0001644 (índice de compensação financeira por dia de atraso, assim apurado

I = (6/100)/365).

CAPÍTULO XIV– DAS SANÇÕES ADMINISTRATIVAS

1. No caso de a licitante, quando convocada, não assinar a ata de registro de preços ou o instrumento contratual, deixar de entregar a documentação exigida neste edital, apresentar documentação falsa, causar o atraso na execução do contrato, não mantiver a proposta dentro do prazo de sua validade, falhar ou fraudar a execução do contrato, comportar-se de modo inidôneo, declarar informações falsas ou cometer fraude fiscal, garantido o direito à ampla defesa, ficará sujeita às penas de impedimento de licitar e contratar com a União e de descredenciamento do SICAF pelo prazo de até 5 (cinco) anos, sem prejuízo das sanções previstas em lei e no contrato (Anexo III).

1.1. A recusa da licitante classificada em assinar a ata de registro de preços ou o contrato no prazo assinalado será considerada como inexecução total da obrigação assumida, ensejando a aplicação das sanções previstas em lei e neste Edital.

1.2. As sanções serão registradas e publicadas no SICAF.

1.3. As sanções descritas no **caput** também se aplicam aos integrantes do cadastro de reserva, que, convocados, não honrarem o compromisso assumido sem justificativa ou com justificativa recusada pela administração.

CAPÍTULO XV– DO REAJUSTE

1. Os preços a serem pagos à **CONTRATADA** pelas licenças descritas nos itens 1, 2 e 3 do lote desta licitação, serão fixos e irreajustáveis pelo período de 12 (doze) meses. Após esse período, o reajuste será feito de ofício, podendo ocorrer negociação entre as partes, momento no qual, será apreciada a possibilidade da aplicação do índice ICTI (IPEA), no período entre o mês básico da apresentação da proposta e o mês anterior ao reajuste, compreendendo sempre o período de 12 meses, de acordo com a seguinte fórmula:

PR =IMR x PA/IMM

Onde:

PR = Preço reajustado

IMR = Índice do ICTI (IPEA) do mês anterior ao reajuste

IMM = Índice do ICTI (IPEA) do mês de apresentação da proposta

PA = Preço anteriormente praticado

2. A administração antes de conceder o reajuste poderá exigir que a contratada apresente planilha demonstrativa com a efetiva variação de seus custos ocorrida no período do reajuste proposto.

CAPÍTULO XVII – DOS CRÉDITOS ORÇAMENTÁRIOS

1. A despesa decorrente do fornecimento/prestação dos serviços objeto deste pregão correrá à conta dos créditos orçamentários consignados à Justiça Eleitoral no Orçamento da União, para o Exercício de 2022, na Natureza de Despesa 33.90.40.06 - Locação de Software, na Ação 02.122.0033.20GP.0001 – PO - Segurança da Informação da Justiça Eleitoral.

CAPÍTULO XVIII – DAS DISPOSIÇÕES FINAIS

1. Em caso de divergência existente entre as especificações descritas no Sistema Comprasnet e as especificações constantes deste Edital, prevalecerão as últimas.

2. Nenhuma indenização será devida às licitantes por apresentarem documentação e (ou) elaborarem proposta relativa ao presente pregão eletrônico.

3. O Tribunal Superior Eleitoral não se responsabilizará por eventuais danos causados à licitante, decorrentes do uso indevido da senha durante as transações efetuadas, ainda que por terceiros.

4. O objeto dos instrumentos contratuais decorrentes deste pregão poderá ser alterado conforme disposto no art. 65 da Lei n° 8.666/93.

5. A existência de preços registrados não obriga a Administração a contratar, facultando-se a realização de licitação específica para a aquisição pretendida, assegurada preferência ao fornecedor registrado em igualdade de condições.

6. A regra é a contratação por lote. A Administração somente poderá contratar cada item que compõe o lote de forma independente, se tiver obtido o menor preço nos lances individuais por item, para aquele item pretendido.

7. Será permitida aos Tribunais Regionais Eleitorais não participantes a adesão à Ata de Registro de Preços proveniente deste Pregão para aquisição dos itens 2 e 3 do Termo de Referência - Anexo I deste Edital.

7.1. O quantitativo decorrente das adesões à ata de registro de preços para os Tribunais Regionais Eleitorais não participantes, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata para o TSE (órgão gerenciador) e para os TREs participantes, independente do número de TREs não participantes que aderirem.

7.2. Não será permitida a adesão de nenhum órgão não participante da ata e não pertencente à Justiça Eleitoral.

8. Caso qualquer documento apresentado pela licitante tenha sido emitido em língua estrangeira, este deverá estar acompanhado da respectiva tradução para a língua portuguesa, efetuada por tradutor juramentado, e devidamente autenticado pela via consular ou registrado em cartório de títulos e documentos, nos termos do Decreto nº 13.609/1943, Lei nº 6.015/73 e demais normas de regência, ressalvado o disposto nos itens 4.10 e 25.9 do Termo de Referência - Anexo I deste Edital.

8.1. Se traduzido para a língua portuguesa no exterior, a tradução deverá ter sido efetuada por profissional qualificado, segundo as leis do país de origem e os documentos autenticados pela via consular.

9. TODOS OS ATOS DO CERTAME DEVEM SER REGISTRADOS EM TEMPO REAL NO SISTEMA COMPRASNET, EXIGÊNCIA QUE NÃO PODERÁ SER AFASTADA EM NENHUMA HIPÓTESE.

10. Conforme disposto no Decreto nº 7.892/2013, as demais licitantes poderão reduzir seus preços ao valor da proposta vencedora para formação de cadastro de reserva. Para tanto, serão adotados os seguintes procedimentos:

10.1. No momento da homologação da licitação, a autoridade competente convocará as licitantes interessadas em fazer parte do cadastro de reserva, informando data/hora fim para formação do cadastro.

10.2. O sistema enviará um e-mail a todos os fornecedores com propostas não recusadas para que eles possam aderir ao Cadastro de Reserva.

10.2.1. Caso seja de interesse, o fornecedor deverá clicar em "PARTICIPAR" para registrar sua intenção em participar do cadastro.

10.3. O cadastro de reserva não prejudicará o resultado do certame em relação à licitante mais bem classificada.

11. Para a aceitabilidade das propostas, das licitantes que aceitaram reduzir seus preços, serão observados os procedimentos definidos no Capítulo VIII deste Edital.

11.1. A habilitação das licitantes que aceitaram reduzir seus preços será efetuada, na hipótese prevista no parágrafo único do art. 13 e quando houver necessidade de contratação de fornecedor remanescente, nas hipóteses previstas nos arts. 20 e 21, do Decreto nº 7.892/2013.

12. As empresas que tenham retirado cópia do edital e seus anexos poderão formular consultas, solicitar informações e obter esclarecimentos relativos à licitação, por escrito, pelo e-mail cpl@tse.jus.br ou nos dias úteis, pelos telefones 3030-8167/8173 da secretaria da Comissão Permanente de Licitação, haja vista as medidas de isolamento preventivas à propagação do novo Coronavírus (COVID-19).

12.1. Qualquer pessoa poderá formular impugnação a este Edital até 3 (três) dias úteis anteriores à data fixada para a abertura da sessão pública, ou seja, até o dia 10 de dezembro de 2021, às 19 horas, inclusive.

12.2. Os pedidos de esclarecimentos referentes a este Edital deverão ser enviados ao pregoeiro até 3 (três) dias úteis anteriores à data fixada para a abertura da sessão pública, ou seja, até o dia 10 de dezembro de 2021, às 19 horas, inclusive.

12.3. As informações, esclarecimentos e respostas a questionamentos, impugnações e recursos serão **obrigatoriamente** publicados no *site* www.comprasgovernamentais.gov.br. e vincularão as licitantes e a Administração.

ADAÍRES AGUIAR LIMA
SECRETÁRIO(A) DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **29/11/2021, às 21:01**, 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=1855772&crc=0376865B, informando, caso não preenchido, o código verificador **1855772** e o código CRC **0376865B**.

TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

EDITAL DE LICITAÇÃO TSE Nº 84/2021

MODALIDADE: PREGÃO

FORMA: ELETRÔNICA

1. OBJETO

1.1. Registro de preços para eventual contratação de subscrições de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento, com pagamento anual, pelo período de 60 meses, consoante especificações, exigências e prazos constantes deste Termo de Referência.

1.2. Farão parte deste Registro de Preços, como órgãos participantes, os Tribunais Regionais Eleitorais – TREs, que serão responsáveis pelas suas respectivas contratações.

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 visa a contratação de uma solução de antivírus que proteja o ambiente computacional da Justiça Eleitoral.

2.4. Tal necessidade decorre pela descontinuidade e encerramento do **Contrato TSE nº 106/2016**, previsto para **1/2/2022**.

2.5. A Justiça Eleitoral possui um parque computacional diversificado, extremamente numeroso e geograficamente espalhado, além de dados que necessitam 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. A Secretaria de Tecnologia da Informação adota, dentre outros, o método de proteção em camadas.

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

2.8. Um moderno software antivírus pode proteger contra: objetos maliciosos Browser Helper (BHOs), sequestradores de navegadores, ransomware, keyloggers, backdoors, rootkits, cavalos de tróia, worms, dialers, fraudtools, adware e spyware. Também incluem proteção contra ameaças virtuais, tais como URLs infectadas e maliciosas, spam, fraude e ataques de phishing, identidade on-line (privacidade), ataques bancários on-line, ameaças persistentes avançadas (APT).

2.9. Devido ao grande número de funcionalidades disponibilizadas pelos atuais fabricantes, a solução de antivírus passou a ser chamada de solução de proteção de estações de trabalho, que pode incluir também proteção a servidores de rede. O termo endpoint também é muito utilizado para se referir a estações de trabalho e notebooks.

2.10. Uma das camadas de proteção é realizada pelo sistema de antimalware, atualmente chamado de sistema de proteção de estações de trabalho (endpoint protection) e datacenter. Esta camada implementa a segurança das estações de trabalho, notebooks, e sistemas de datacenters, oferecendo proteção em tempo real contra as ameaças mais comuns da Internet como vírus, worms, trojans e ransomwares, além de fornecerem opções avançadas de segurança como o bloqueio de dispositivos e análise de ameaças não conhecidas chamadas de 0 Day.

2.11. Seguindo as tendências de evolução de atividades maliciosas, vale ressaltar também o processo evolutivo das soluções de proteção ao ambiente. Atualmente a proteção de EDR, aliada a proteção de endpoint, se tornou um requisito mínimo para proteção adequada do ambiente, provendo maior capacidade de detecção e principalmente de resposta a atividades maliciosas em endpoints.

2.12. Em 2017 o Centro de Tratamento de Incidentes de Redes do Governo (CTIR Gov) por meio do "Alerta nº 07/2017- Ataques de Ransomware Bad Rabbi" reforçou a necessidade de manutenção dos softwares de antivírus para todos os órgãos e entidades da administração pública, tal medida visa mitigar as ameaças de sequestro de dados.

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

2.14. A natureza desta contratação tem fundamento na Lei nº 10.520/2002, no Decreto nº10.024/2019 e nos termos da Lei 8.666/1993.

2.15. 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.

2.16. 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.

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

2.18. 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.

2.19. Por fim, tendo em vista que a demanda em questão visa garantir a segurança, proteção, integridade e autenticidade das informações, entende-se necessária a contratação de aquisição da solução de antivírus, a fim de que haja a continuidade dos serviços de forma a assegurar o cumprimento da missão institucional da Justiça Eleitoral.

2.20. Isto posto, esta equipe técnica propõe a contratação de subscrições de solução de segurança pelo período de 60 (sessenta) meses, sendo que os pagamentos das subscrições ocorrerão a cada 12 meses.

2.21. 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 1831004).

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1. DESCRIÇÃO DAS SUBSCRIÇÕES E SERVIÇOS A SEREM EXECUTADOS

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

3.3. A licitante deverá encaminhar proposta de preços especificando marca e modelo do produto ofertado.

3.4. Não será aceita a utilização de software livre na composição das subscrições de solução de antivírus com EDR.

4. CONDIÇÕES GERAIS

4.1. A forma de cumprimento de qualquer requisito explicitado no objeto deverá ser detalhadamente descrito, com menção a limitações e restrições que existirem e de trechos da literatura técnica correspondente, e onde se encontram referências relevantes ao assunto.

4.2. A instalação de qualquer componente fornecido neste objeto deverá prever a aplicação de todas as correções publicadas e divulgadas pelo fabricante, durante a vigência das subscrições.

4.3. Caso a solução necessite de banco de dados específico e proprietário para funcionamento da solução, as licenças deste deverão ser fornecidas pela contratada junto com a solução ofertada sem ônus para o contratante, além daquele já cotado em sua proposta.

4.4. As licenças de sistema operacional e do ambiente de virtualização, bem como o equipamento para execução da solução serão fornecidos pelo Contratante.

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

4.6. Para prestação do suporte técnico, a Contratada deverá sempre alocar empregados qualificados e com a devida certificação técnica no produto.

4.7. A Contratada será responsável pela entrega das subscrições, no prazo máximo de 30 (trinta) dias corridos e contados do início da vigência do contrato. As licenças deverão ser entregues em formato digital, para o e-mail sesap@tse.jus.br, ou para download em site do fabricante do produto.

4.8. Os documentos técnicos deverão ser apresentados junto com a proposta, por planilha contendo item, a descrição do item, e a comprovação técnica de atendimento.

4.9. As especificações das características técnicas da solução de segurança ofertada deverão estar descritas de forma clara e detalhada.

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

4.11. As licenças deverão possuir data de validade à partir do recebimento definitivo efetuado pelo Contratante.

4.11.1. A validade usual de mercado deve ser comprovada, sendo de, no mínimo, 72 (setenta e dois) meses, contados da data de fabricação, não podendo ter transcorrido mais de 30 (trinta) dias do prazo de validade no momento da entrega.

4.12. O endereço da sede do TSE fica situado na SAFS Quadra 7 Lotes 1/2, Brasília/DF, de segunda a sexta-feira, entre 10 e 19 horas.

4.13. A instalação de todos os 28 (vinte e oito) sítios, configuração e ativação das subscrições deverá ocorrer e ser concluída em até 35 (trintas) dias após o início da vigência contratual.

4.14. Nos 30 (trinta) dias que antecederem o vencimento das subscrições a contratada deverá providenciar a renovação das mesmas, com validade à partir do vencimento das subscrições ativas.

4.15. As subscrições renovadas devem ser entregues e ativadas, no máximo, até o vencimento das subscrições em uso de modo a não haver interrupção nos serviços.

4.16. Cabe a Contratada ativar as subscrições na ferramenta instalada.

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

5. NATUREZA DO OBJETO

5.18. Trata-se de objeto com características comuns e usuais encontradas no mercado de TIC, cujos padrões de desempenho e de qualidade podem ser objetivamente definidos, enquadrados nos termos da Lei n.º 10.520/2002 e do Decreto n.º 10.024/2019.

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

6.1. O quantitativo solicitado está relacionado no **ANEXO I-VII - QUANTIDADES ESTIMADA PELOS TREs E TSE,** proveniente de levantamento realizado junto aos Regionais.

6.2. Em virtude das especificidades existentes em cada Tribunal Regional Eleitoral, sugerimos que seja dada a permissão para que os Tribunais Regionais Eleitorais possam realizar adesões à Ata de Registro de Preços proveniente da licitação do objeto deste Termo de Referência para aquisição dos itens 2 e 3, respectivamente, conforme Ofício Circular nº 335 Gab-DG, SEI 1822477.

6.3. Da mesma forma, atender ao que é estabelecido no Art. 1º da Resolução 396 CNJ (1676014), Parágrafo Único, assim como ao Relatório - Estratégia Nacional de Cibersegurança v2 (1759818), no qual consta a necessidade de aquisição de ferramentas automatizadas para governança e continuidade do negócio.

7. PARCELAMENTO DO OBJETO

7.1. A solução é composta dos seguintes itens:

Lote	Item	Descrição
1	**1**	Solução de segurança de EndPoint (**desktops**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.
	2	Solução de Segurança de EndPoint (**desktops)**, com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.
	3	Solução de Segurança para Servidores (**Linux e Windows**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).
	5	Transferência de conhecimento (parcela única).

7.2. A adjudicação se dará para um único fornecedor, logo, não será aceita a composição entre múltiplos fabricantes para atendimento das especificações deste Termo de Referência.

8. SUPORTE TÉCNICO:

8.1. O Suporte Técnico deve ser prestado durante todo o período de validade das subscrições.

8.2. Os serviços de suporte pertinentes aos **itens 1, 2 e 3** deverão ser realizados por técnicos do fabricante ou por técnicos da Contratada, certificados na solução.

8.3. Deverá ser executado pelo fabricante da solução ou por técnico da Contratada e deverá englobar solução de problemas nas ferramentas fornecidas, inclusive ajustes na configuração e ajustes de regras para melhor detecção de vírus e malwares, por técnico dedicado em português, a ser prestado no regime 8x5 (oito horas por dia, cinco dias por semana), durante horário comercial.

8.4. Em caso de incidentes considerados graves, como por exemplo: ataques direcionados à Justiça Eleitoral, ataques ransonware, epidemias (cavalo de Troia, Adware, Script, Backdoor, Stealth, Boot), o referido suporte deverá ser prestado em regime 24 x 7 (vinte e quatro horas por dia, sete dias por semana).

8.5. O tempo máximo para início do atendimento a chamados é de 1 (uma) hora, contados do recebimento da notificação do Contratante.

8.6. O tempo máximo para implementação de solução definitiva ou de contorno para problemas é de 6 (seis) horas, contados do recebimento da notificação do Contratante.

8.7. Caso o problema seja bug da ferramenta a contratada deverá acordar uma data e prazo com o Contratante para resolução de problema.

8.8. 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.

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

8.10. A Contratada deve realizar ajustes nas políticas da solução de antivírus sempre que a equipe técnica do Contratante entender conveniente.

8.11. Sempre que houver incidentes relacionados a vírus, o contratante poderá solicitar à Contratada que realize ajustes na ferramenta.

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

8.13. Deverão ser fornecidas obrigatória e automaticamente todas as atualizações de versão que ocorrerem durante toda a vigência das subscrições.

8.14. A Contratada deve executar o objeto deste projeto em conformidade com as determinações do fabricante da solução, utilizando-se das melhores práticas para configuração da solução, e, ainda, de acordo com as instruções emitidas pelo Contratante, quando for o caso.

8.15. A Contratada deve garantir que novas versões de software ou atualizações dos produtos em garantia tenham a perfeita compatibilidade com o ambiente operacional em uso nas instalações do Contratante.

8.15.1. O prazo de garantia deverá ser de, no mínimo, 60 (sessenta) meses, contados da data do recebimento definitivo.

8.15.2. O prazo para substituição das subscrições que apresentarem defeito durante o prazo de garantia deverá ser de até 2 (dois) dias úteis, contados do recebimento da notificação do Contratante.

8.15.3. O custo e a responsabilidade pelo recolhimento e entrega do produto durante o prazo de garantia serão da CONTRATADA.

8.16. Caso o Contratante decida pelo atendimento remoto, o mesmo deve ser prestado diretamente pelos profissionais da Contratada ou do fabricante, através da plataforma de suporte remoto a ser definido pelo Contratante.

8.17. A solução deve proteger os usuários contra *exploits* baseados na Web que tenham como alvo aplicativos vulneráveis, como navegadores da Web, Microsoft Office e Adobe Reader, para descarregar um conteúdo de malware no disco e iniciá-lo.

8.18. A solução deve evitar que aplicativos de alto risco (como navegadores ou manipuladores de documentos) iniciem processos secundários não confiáveis, carreguem dlls não confiáveis ou explorem o PowerShell em ataques com base em conteúdo.

9. NÍVEIS DE SERVIÇO

9.1. O atendimento aos chamados deverá estar disponível de segunda-feira a sexta-feira, no horário das 9h às 17h, horário de Brasília. A abertura de chamados pelo Contratante será efetuada por correio eletrônico, por sistema de controle de chamados ou por telefone. A abertura de chamado poderá ocorrer em qualquer horário por e-mail ou sistema de controle de chamados, enquanto por telefone apenas no horário mencionado. No caso de abertura de chamado fora do horário estipulado, a contagem do prazo, para efeitos de nível de serviço (SLA), se dará no próximo dia útil;

9.1.1. A CONTRATADA deverá confirmar que recebeu a solicitação de chamado, para fins de contagem do prazo, através de resposta automática de confirmação de e-mails recebidos, relatório de sistema de chamado ou e-mail de envio de protocolo de chamados abertos via central telefônica;

9.2. A assistência técnica em garantia deve garantir o fornecimento de acesso irrestrito (24 horas x 7 dias da semana) à área de suporte do fabricante, especialmente ao endereço eletrônico (web site), a toda a documentação técnica pertinente (guias de instalação/configuração atualizados, FAQ's, bases de conhecimento e bases de soluções, com pesquisa efetuada através de ferramentas de busca);

9.3. O suporte técnico do fabricante deverá ser prestado em caso de falhas, dúvidas e/ou esclarecimentos de qualquer um dos itens (produtos, módulos e software) que compõem a solução;

9.4. Os serviços de suporte deverão ser corretivos, proativos e consultivos, envolvendo atividades como auxílio na configuração de políticas e administração da solução, instalação de novas versões, patches e hotfixes, análise de dúvidas sobre melhores práticas de configuração, entre outros;

9.5. Os prazos de resposta para problemas ocorridos durante o período de suporte estão apresentados na tabela abaixo e são contados do recebimento da notificação de abertura do chamado:

Grau de impacto	Descrição	Tempo máximo para resposta inicial	Tempo máximo para solução definitiva ou de contorno para problemas
Nível 1 - Alto	• Indisponibilidade de uso da solução	1 hora comercial	8 horas
Nível 2 - Médio	• Falha, simultânea ou não, de uma ou mais funcionalidades que não cause indisponibilidade, mas apresente problemas de funcionamento e/ou performance da solução	2 horas comerciais	1 dia útil
Nível 3 - Baixo	• Instalação, configuração, atualização de versões e implementações de novas funcionalidades	4 horas comerciais	2 dias úteis

9.6. Automaticamente e sem custos adicionais, deverá ser possível o acesso ao conteúdo mais recente dos produtos, funcionalidades adicionais e correções de produtos disponibilizadas pelo fabricante;

9.7. A CONTRATADA deverá manter, durante toda a vigência do prazo de garantia, um "gerente técnico de contas". O "gerente técnico de contas" deverá ser o ponto de contato entre o FABRICANTE, CONTRATADA e CONTRATANTE para solucionar pendências e questões que não foram resolvidas pelo suporte técnico.

10. CRONOGRAMA DE EXECUÇÃO

10.1. 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	Assinatura do contrato	CONTRATANTE e CONTRATADA	Contrato assinado.
D+5	Reunião de Planejamento	CONTRATANTE e CONTRATADA	Ata de reunião assinada.
D+35	Concluir instalação e configuração da solução nos 28 sítios	CONTRATADA	Solução implantada e funciona plenamente.
D+45	Recebimento Provisório	CONTRATANTE	Parecer do Fiscal Técnico.
D+50	Recebimento Definitivo	CONTRATANTE	Verificação do funcionamento e especificações dos produtos e se entregues.

11. RECEBIMENTO

11.1. Para os itens 1, 2 e 3:

11.1.1. Recebimento Provisório

11.1.2. Em até 2 (dois) dias corridos após a entrega das subscrições, acompanhadas das respectivas Notas Fiscais, será emitido o Termo de Recebimento Provisório - TRP, por servidor ou comissão previamente designados.

11.2. Recebimento Definitivo

11.2.1. Após a ativação das subscrições, que deverá ser realizada em até 5 (cinco) dias úteis após a entrega das subscrições, o fiscal terá o prazo de 10 (dez) dias corridos para emitir o Termo de Recebimento Definitivo - TRD, e remeter o processo ao fiscal administrativo. O TRD se dará em conformidade com o descrito no Anexo I-III deste Termo de Referência.

11.2.2. 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.

11.2.3. A Contratada deverá refazer ou corrigir os serviços não aprovados pela fiscalização e cumprir as obrigações pendentes em até 5 (cinco) dias corridos, contados da notificação.

11.2.4. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reaberto novo prazo para emissão do TRD.

11.2.5. 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.

11.3. Para o item 4:

11.3.1. Recebimento Provisório

11.3.2. Em até 2 (dois) dias corridos após a implantação da solução em todos os sítios, acompanhadas das respectivas Notas Fiscais, será emitido o Termo de Recebimento Provisório - TRP, por servidor ou comissão previamente designados.

11.4. Recebimento Definitivo

11.4.1. Após a conclusão da instalação da solução em todos os sítios, 28 (vinte e oito), o fiscal terá o prazo de 10 (dez) dias corridos para emitir o Termo de Recebimento Definitivo - TRD, e remeter o processo ao fiscal administrativo. O TRD se dará em conformidade com o descrito no Anexo I-III deste Termo de Referência.

11.4.2. Para o item 5:

11.5. Recebimento Provisório

11.5.1. Em até 2 (dois) dias corridos após a entrega Nota Fiscal, será emitido o Termo de Recebimento Provisório - TRP, por servidor ou comissão previamente designados.

11.6. Recebimento Definitivo

11.6.1. Após o recebimento do Questionário de Avaliação (item 25.11 do Anexo I-I), o fiscal terá o prazo de 10 (dez) dias corridos para emitir o Termo de Recebimento Definitivo - TRD, em duas vias, e remeter o processo ao fiscal administrativo.

11.6.2. 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.

11.6.3. A Contratada deverá refazer ou corrigir os serviços não aprovados pela fiscalização e cumprir as obrigações pendentes em até 5 (cinco) dias corridos, contados da notificação.

11.6.4. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reaberto novo prazo para emissão do TRD.

11.6.5. 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.

12. PAGAMENTO

12.1. Para os itens 1, 2 e 3:

12.1.1. O pagamento ocorrerá *anualmente*, conforme disposto no item 1.1 deste Termo de Referência.

12.1.2. O pagamento será efetuado até o 10º (décimo) dia útil, a partir do atesto da 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.

12.1.3. Este procedimento de pagamento é válido para o pagamento das subscrições e para suas renovações anuais.

12.1.4. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento no ato da entrega do objeto e quando das renovações anuais das subscrições.

12.2. Para o item 4:

12.2.1. Será realizado em parcela única e somente após a conclusão das 28 (vinte e oito) instalações do software de gerência da solução.

12.2.2. O pagamento será efetuado até o 10º (décimo) dia útil, a partir do atesto da 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.

12.2.3. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento após a implantação completa da solução no TSE e demais 27 Tribunais Regionais Eleitorais.

12.3. Para o item 5:

12.3.1. Será realizado em parcela única e efetuado até o 10º (décimo) dia útil, a partir do atesto da 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.

12.3.2. A Contratada deverá entregar o faturamento com toda documentação exigida para liquidação e pagamento em até 2 (dois) dias úteis após a realização da transferência de conhecimento.

12.4. O atesto do objeto contratado se dará pelo fiscal, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto - NTA. O fiscal terá o prazo de 2 (dois) dias úteis para emitir a NTA e remeter o processo a 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.

13. OBRIGAÇÕES DA CONTRATADA

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

13.2. Responsabilizar-se pelas despesas decorrentes do fornecimento dos produtos e da execução dos serviços objetos deste Termo de Referência.

13.3. Informar, no momento da formalização do instrumento contratual, nome do responsável (preposto), 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.

13.4. 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.

13.5. 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 conta de e-mail.

13.6. 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.

13.7. Acatar as recomendações efetuadas pelo fiscal do contrato.

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

13.9. 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.

13.10. 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).

13.11. 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.

13.12. 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.

13.13. Manter, durante a execução do contrato as condições de habilitação exigidas na licitação.

13.14. Verificadas irregularidades nas condições que ensejaram sua habilitação quanto à regularidade fiscal, a contratada terá o prazo de 30 (trinta) dias corridos, contados da notificação da fiscalização, para regularizar a situação, sob pena de aplicação das penalidades cabíveis, sem prejuízo da rescisão do contrato a critério da Administração.

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

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

13.17. O Preposto, em nome da contratada, e todos os demais funcionários que atuarem na execução da contratação deverão assinar o Termo de Confidencialidade, conforme Anexo I-V deste Termo de Referência.

14. OBRIGAÇÕES DO CONTRATANTE

14.1. Prestar as informações e os esclarecimentos que venham a ser solicitados pela contratada.

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

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

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

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

14.6. Receber a Contratada para reunião inaugural, conforme prazo definido no item 10.1 (Cronograma de Execução).

14.7. Efetuar o pagamento à contratada, segundo as condições estabelecidas nesse Termo de Referência.

15. PREÇOS ESTIMADOS

Lote	Item	Descrição	Preço Unitário (R$)	Preço Total (60 meses) (R$)
1	**1**	Solução de segurança de EndPoint (**desktops**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. **Qtde Registrada: 35.906**	R$ 281,95 (por 60 meses)	R$ 10.123.696,7(
	2	Solução de Segurança de EndPoint (**desktops**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. **Qtde Registrada: 21.077**	R$ 415,00 (por 60 meses)	R$ 8.746.955,00
	3	Solução de Segurança para Servidores (**Linux e Windows**, com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. **Qtde Registrada: 8.360**	R$ 605,00 (por 60 meses)	R$ 5.057.800,00
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única). **Qtde Registrada: 28**	R$ 12.213,87 (parcela única)	R$ 341.988,36
	5	Transferência de conhecimento (parcela única). **Qtde Registrada: 4 Turmas**	R$ 22.250,00 (parcela única)	R$ 89.000,00
			PREÇO TOTAL DO LOTE	**R$ 24.359.440,0**

16. PRAZO DE VIGÊNCIA DO CONTRATO

16.1. O(s) contrato(s) oriundo(s) da ARP terá(ão) vigência a partir de ____ de _____ de 202___ e duração de até 60 (sessenta) meses.

17. SUBCONTRATAÇÃO

17.1. É vedado à Contratada transferir a outrem a parcela de maior relevância do objeto da presente licitação. Todavia, fica permitida a subcontratação do próprio fabricante, para execução dos serviços de suporte técnico.

17.2. A subcontratação só será autorizada pelo CONTRATANTE após a comprovação da capacidade técnica da empresa para executar os serviços pretendidos e de sua regularidade fiscal.

18. CONSÓRCIO

18.1. É vedada a participação em consórcio.

18.2. Durante a elaboração deste projeto foi constatado 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 representaria restrição à competição.

19. CRITÉRIOS DE SUSTENTABILIDADE

19.1. Comprovação, como condição de participação na licitação, 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 Ministério do Trabalho e Previdência, atualizada periodicamente em seu sítio eletrônico (https://www.gov.br/trabalho/pt-br/assuntos/fiscalizacao/combate-ao-trabalho-escravo).

19.1.1. Deverá ser apresentada a Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa") **da Justiça Federal e da justiça comum** para a licitante e seus dirigentes.

19.2. Comprovação, como condição de participação na licitação, 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. 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 contratada e seus dirigentes.

19.3. Na especificação dos bens adotou-se como medida sustentável a obrigação da contratada fornecer as subscrições em meio digital.

ANEXO I-I - ESPECIFICAÇÕES TÉCNICAS

20. REQUISITOS GERAIS DA GERÊNCIA INTEGRADA DE SEGURANÇA – COMUNS AOS ITENS 1, 2 e 3:

20.1. A Gerência Integrada deve estar disponível para instalação On-Premise ou utilização em nuvem própria do fabricante;

20.2. A Gerência Integrada deve prover a administração dos produtos/componentes (políticas, relatórios) com suas funções e módulos gerenciando as tecnologias: tais como: criptografia, blindagem das vulnerabilidades, EDR, antimalware e Sandbox;

20.3. A Gerência Integrada deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

20.4. A Gerência Integrada deve possuir capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

20.5. Todos os módulos/aplicações que compõem a solução devem ser do mesmo fabricante:

20.5.1. Para o caso de appliance virtual, deverá suportar, no mínimo, o Hypervisor VMWare vSphere 6.7 ou superior;

20.5.2. Para o caso de instalação em sistema operacional Windows, deverá ser compatível, no mínimo, com a versão Microsoft Windows Server 2008 e superior;

20.6. A solução deve possuir Gerência Integrada com acesso via WEB (HTTPS) ou MMC (Microsoft Management Console);

20.7. A Gerência integrada deve prover:

20.7.1. Painel para monitoramento;

20.7.2. Capacidade de criação de relatórios;

20.7.3. Mecanismo para envio de notificações administrativas (e–mail);

20.7.4. Possibilidade de customização do painel de monitoração através de widgets;

20.7.5. Possibilidade de geração de relatórios customizados com diversas informações, tais como: tipos de infecção, máquinas infectadas, vírus detectados, ações tomadas, quantidade de infecções, dentre outros.

20.8. Deve permitir visualizar o status de assinaturas de segurança dos dispositivos gerenciados pela solução;

20.9. A Gestão Integrada deve mostrar quantos dispositivos estão sendo gerenciados e quais seus sistemas operacionais;

20.10. Deve possuir a capacidade de autenticação dos usuários do console de gerenciamento através do Microsoft Active Directory.

20.10.1. Deve permitir a definição de perfis com diferentes níveis de privilégios de administração da solução, baseados em usuários ou grupos do Microsoft Active Directory;

20.10.2. Capacidade de exportar relatórios para, no mínimo, dos seguintes tipos de arquivos: PDF, HTML e CSV;

20.10.3. Capacidade de enviar e–mails para contas específicas, em caso de algum evento;

20.10.4. A Gestão Integrada deve fornecer as seguintes informações dos computadores protegidos:

20.10.4.1. Horário da última conexão da máquina com o servidor administrativo ou, no mínimo, o tempo decorrido desde a última conexão;

20.10.4.2. Data e horário da última verificação executada na máquina;

20.10.4.3. Se a solução está instalada;

20.10.4.4. Versão do antivírus instalado na máquina gerenciada;

20.10.4.5. Se o antivírus está atualizado;

20.10.4.6. Nome do computador;

20.10.4.7. Domínio ou grupo de trabalho do computador;

20.10.4.8. Sistema operacional;

20.10.4.9. Endereço IP;

20.10.4.10. Aplicativos instalados;

20.11. Capacidade de instalar remotamente a solução nas estações e servidores Windows, através da Gerência Integrada, ou GPO do Microsoft Active Directory;

20.12. Capacidade de gerar pacotes auto−executáveis para a instalação do software para gerenciamento, além de automatização para instalação de todos os módulos e informações necessárias para o funcionamento do produto (licenças, configurações);

20.13. Capacidade de importar a estrutura do Microsoft Active Directory para a descoberta de máquinas da rede corporativa;

20.14. Capacidade de monitorar a rede, em diferentes sub redes, a fim de encontrar máquinas novas, para a instalação automática ou através de script(GPO);

20.15. Deve ser capaz de eleger qualquer computador Desktop ou Servidor como repositório de vacinas e de hotfix, sem a necessidade de instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar o tráfego da rede;

20.16. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar o tráfego;

20.17. Deve permitir a herança de tarefas e políticas na estrutura de hierarquia de servidores administrativos;

20.18. Capacidade de realizar atualização incremental de vacinas nos computadores clientes a partir da rede local e da Internet;

20.19. A atualização incremental de vacinas deve ser disponibilizada, no mínimo, com frequência diária;

20.20. A solução deve possuir integração com o Active Directory, de maneira a permitir a definição de políticas diferentes, baseadas em usuários ou grupos;

20.21. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;

20.22. Deve armazenar histórico das alterações feitas em políticas;

20.23. Deve permitir a realocação de máquinas novas na rede para um determinado grupo utilizando os parâmetros ou através de algoritmo próprio;

20.23.1. Nome do computador;

20.23.2. Range de IP;

20.23.3. Sistema Operacional;

20.24. Caso a solução ofertada não atenda na totalidade os itens aqui referidos, será permitido a composição com outras soluções a fim de atender na plenitude dos itens aqui descritos, garantindo que a solução composta seja do mesmo fabricante.

20.25. Deve possuir uma base de inteligência global, do próprio fabricante, sobre ameaças existentes;

20.26. Deve ser capaz de dar visibilidade sobre ameaças globais;

20.27. A solução deve ser capaz de proporcionar a busca por ameaças baseadas em IOCs;

20.28. Deve ser capaz de indicar quantos e quais dispositivos dentro da empresa estão vulneráveis a determinada ameaça;

20.29. Deve ser capaz de mostrar o nível de postura de segurança da organização, em relação às políticas aplicadas no ambiente protegido.

20.30. Cada ameaça identificada pela solução deverá possuir as seguintes informações:

20.30.1. Detalhes do ataque;

20.30.2. IOCs;

20.30.3. Detalhes do Impacto no ambiente;

20.30.4. Endpoints afetados;

20.30.5. Comportamento da ameaça.

21. ITEM 1 - SOLUÇÃO DE SEGURANÇA DE ENDPOINT (DESKTOPS), COM EDR E SANDBOX

21.1. Requisitos Gerais

21.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado;

21.1.2. Se comunicar com a Gerência Integrada da solução, de forma que seja possível gerenciar todas as funcionalidades;

21.1.3. Detectar e eliminar programas maliciosos (malwares), tais como vírus, ransomware, spywares, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

21.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;

21.1.5. Deve detectar e eliminar programas maliciosos em:

21.1.5.1. Processos Em Execução Em Memória principal (RAM);

21.1.5.2. Arquivos Executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

21.1.5.3. Arquivos Compactados, em tempo real ou no ato de sua execução, com os seguintes formatos: ZIP, EXE, ARJ, RAR, e CAB;

21.1.5.4. Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

21.1.6. Capacidade de detecção heurística de malwares desconhecidos;

21.1.7. Possuir tecnologia de Machine Learning de pre- execution, run time machine e post- execution;

21.1.8. Deve prover, no mínimo, as seguintes proteções:

21.1.8.1. Antivírus de arquivos;

21.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);

21.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System);

21.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;

21.1.8.5. Controle de dispositivos;

21.1.8.6. Controle de execução de arquivo e aplicativos também por meio hash;

21.1.8.7. Bloqueio de sites maliciosos categorizados de acordo com a nuvem do fabricante;

21.1.8.8. Prevenção contra exploração de vulnerabilidades.

21.1.8.9. Capacidade de integração com a Antimalware Scan Interface (AMSI);

21.1.8.10. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

21.1.8.11. Controle de vulnerabilidades do Windows e de softwares de terceiros instalados;

21.1.8.12. Capacidade de instalar correções, de forma manual e automática, das vulnerabilidades de acordo com a severidade;

21.1.8.13. Capacidade de gerenciar as políticas de bloqueio de vulnerabilidades, fazendo o deploy das regras de acordo com as características do dispositivo;

21.2. Detalhamento das proteções:

21.2.1. Antivírus de arquivos:

21.2.1.1. Verificar todos os arquivos criados, acessados ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;

21.2.1.2. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando–as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

21.2.1.3. Deve possuir Módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

21.2.1.4. Deve possuir Módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro;

21.2.1.5. Deve possuir módulo que analise qualquer tentativa maliciosa de edição, exclusão ou gravação do registro;

21.2.1.6. Capacidade para definir escopo de varredura/rastreamento: todos os discos locais, discos específicos;

21.2.1.7. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí–los da verificação;

21.2.1.8. Possibilidade de definir frequência de varredura;

21.2.1.9. Capacidade de realizar a verificação "inteligente" de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá–la apenas a partir da extensão do arquivo;

21.2.1.10. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

21.2.2. Antivírus web:

21.2.2.1. Possuir módulo de web-antivírus para proteção contra ameaças durante navegação na internet;

21.2.2.2. Capacidade de limitar o acesso a sites da internet por reputação ou categorização;

21.2.2.3. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web;

21.2.2.4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Mozilla Firefox e Google Chrome.

21.2.3. Firewall de host com HIPS e/ou HIDS

21.2.3.1. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:

21.2.3.2. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas ou, definir o comportamento da filtragem de pacotes, podendo definir pelo menos, mas não limitado a permitir, bloquear ou bloquear com exceções aos pacotes de rede;

21.2.3.3. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso à rede;

21.2.3.4. Deve possuir módulo HIPS e/ou HIDS para proteção/detecção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

21.2.4. Proteção contra Ameaças Avançadas

21.2.4.1. A solução deve permitir a análise comportamental avançada de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware);

21.2.4.2. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas permitindo sua execução e analisando seu comportamento no endpoint;

21.2.4.3. Deve permitir criar exceções para aplicações confiáveis, evitando que sejam bloqueadas por componentes de detecção;

21.2.4.4. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;

21.2.4.5. Solução deve manter um cache de reputação local com informações de aplicações conhecidas, desconhecidas e maliciosas;

21.2.4.6. Dentre os comportamentos maliciosos, deve ser capaz de "bloquear" ou "detectar e trazer rastreabilidade sobre":

21.2.4.7. Acesso local a partir de cookies;

21.2.4.8. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

21.2.4.9. Criação de threads em outro processo;

21.2.4.10. Desativação de executáveis críticos do sistema operacional;

21.2.4.11. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

21.2.4.12. Gravação e Leitura na memória de outro processo;

21.2.4.13. Modificação da política de firewall do Windows;

21.2.4.14. Modificação da pasta de tarefas do Windows;

21.2.4.15. Modificação de arquivos críticos do Windows e Locais do Registro;

21.2.4.16. Modificação de arquivos executáveis portáteis;

21.2.4.17. Modificação de bit de atributo oculto;

21.2.4.18. Modificação de bit de atributo somente leitura;

21.2.4.19. Modificação de entradas de registro de DLL AppInit;

21.2.4.20. Modificação de locais do registro de inicialização;

21.2.4.21. Modificação de pastas de dados de usuários;

21.2.4.22. Modificação do local do Registro de Serviços;

21.2.4.23. Suspensão de um processo;

21.2.4.24. Deve ser capaz de bloquear ou apenas informar quando uma ameaça for encontrada;

21.2.4.25. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem;

21.2.4.26. Deve possuir modo de ativação da análise comportamental avançada para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

21.2.4.27. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

21.2.4.28. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

21.2.4.29. Utilizar técnicas de machine learning para detecção de ameaças.

21.2.4.30. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

21.2.5. Criptografia

21.2.5.1. Características

21.2.5.2. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

21.2.5.3. Deve ser compatível com sistemas operacionais Desktop Windows;

21.2.5.4. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

21.2.5.5. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

21.2.5.6. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

21.2.5.7. Permitir criar vários usuários de autenticação pré-boot;

21.2.5.8. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

21.2.5.9. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

21.2.5.10. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

21.2.5.11. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

21.2.5.12. Criptografar todos os arquivos individualmente;

21.2.5.13. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

21.2.5.14. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

21.2.5.15. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente.

21.2.5.16. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

21.2.5.17. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

21.2.5.18. Capacidade de verificar a compatibilidade de hardware antes de aplicar a criptografia;

21.2.5.19. Possibilitar estabelecer parâmetros para a senha de criptografia;

21.2.5.20. Capacidade de permitir ao usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

21.2.5.21. Permitir criar exclusões para não criptografar determinados "discos rígidos" através de uma busca por nome do computador ou nome do dispositivo

21.2.5.22. Permitir criptografar as seguintes pastas pré-definidas: "meus documentos", "Favoritos", "Desktop", "Arquivos temporários" e "Arquivos do outlook";

21.2.5.23. Permitir utilizar variáveis de ambiente para criptografar pastas customizadas;

21.2.5.24. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio;

21.2.5.25. Permitir criar um grupo de extensões de arquivos a serem criptografados;

21.2.5.26. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

21.2.5.27. Permitir criptografia de dispositivos móveis (Notebooks) quando o endpoint não possuir comunicação com a console de gerenciamento;

21.2.5.28. Capacidade de deletar arquivos de forma segura após a criptografia;

21.2.5.29. Capacidade de criptografar somente o espaço em disco utilizado;

21.2.5.30. Deve ter a opção de criptografar arquivos criados a partir de aplicações ou extensões selecionadas pelo administrador;

21.2.5.31. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;

21.2.5.32. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo;

21.2.5.33. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

21.2.5.34. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

21.2.5.35. Capacidade de fazer "Hardware encryption";

21.2.6. Controle de dispositivos:

21.2.6.1. Deve possuir módulo de controle de dispositivos, que permita o bloqueio e a ativação de dispositivos, no mínimo as seguintes categorias:

21.2.6.2. Discos de armazenamento locais;

21.2.6.3. Armazenamento removível;

21.2.6.4. Impressoras;

21.2.6.5. CD/DVD;

21.2.6.6. Drives de disquete;

21.2.6.7. Modems;

21.2.6.8. Dispositivos multifuncionais;

21.2.6.9. Leitores de Smart Card;

21.2.6.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile);

21.2.6.11. Wi-Fi;

21.2.6.12. Adaptadores de rede externos;

21.2.6.13. Dispositivos MP3 ou smartphones;

21.2.6.14. Dispositivos Bluetooth;

21.2.6.15. Câmeras e Scanners.

21.2.6.16. Capacidade de liberar o acesso a um dispositivo especıfico sem a necessidade de desabilitar a proteção ou da intervenção local na máquina do usuário;

21.2.6.17. Capacidade de adicionar novos dispositivos por Class ID/Hardware ID.

21.2.7. Controle de execução de aplicativos:

21.2.7.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

21.2.7.2. Deve ser capaz de realizar varredura nas estações de trabalho protegidas informando as aplicações presentes;

21.2.7.3. Como resultado da varredura, a solução deve armazenar o nome completo da aplicação, checksum, nome da aplicação ou versão da aplicação e fabricante;

21.2.7.4. Ao detectar um executável, a solução deverá consultar a solução de reputação de arquivos e compartilhamento de informações de segurança;

21.2.7.5. Ao detectar uma aplicação, deverá consultar a solução de reputação de arquivos e compartilhamento de informações de segurança;

21.2.7.6. Caso não seja possível efetuar comunicação com a solução de reputação de arquivos e compartilhamento de informações de segurança, o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;

21.2.7.7. Deve ser possível criar uma imagem base para a criação de uma política geral;

21.2.7.8. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando−se à novas aplicações instaladas na máquina;

21.2.7.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA− 1);

21.2.7.10. A solução deve suportar as seguintes modalidades de proteção:

21.2.7.11. Criação de uma lista de aplicações autorizadas que podem ser executadas, onde todas as demais aplicações são impedidas de serem executadas;

21.2.7.12. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;

21.2.7.13. Monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

21.2.7.14. Deve ser capaz de proteger em modo standalone − online ou offline;

21.2.7.15. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize−as de forma a adaptar a necessidade do órgão;

21.2.7.16. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

21.2.7.17. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

21.2.7.18. Permitir monitoração de Hooking de aplicações;

21.2.8. Proteção contra ransomwares:

21.2.8.1. Bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado em outra máquina;

21.2.8.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;

21.2.8.3. Na detecção de atividade maliciosa de criptografia por ransomware, o antivírus deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

21.3. Compatibilidade

21.3.1. O software de proteção deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:

21.3.2. Microsoft Windows 8.1 (e suas edições);

21.3.3. Microsoft Windows 10 (e suas edições);

21.3.4. Ser compatível para instalação em sistemas legados em Windows 7 (e suas edições).

21.3.5. O software de proteção deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:

21.3.5.1. Microsoft Windows Server 2008 R2 (e suas edições);

21.3.5.2. Microsoft Windows Server 2012 (e suas edições);

21.3.5.3. Microsoft Windows Server 2012 R2 (e suas edições);

21.3.5.4. Microsoft Windows Server 2016 (e suas edições);

21.3.5.5. Microsoft Windows Server 2019 (e suas edições).

21.4. Sandbox

21.4.1. Compatibilidade

21.4.1.1. A solução de SandBox deverá suportar utilização em nuvem própria do fabricante ou em ambiente computacional da Justiça Eleitoral;

21.4.1.2. Pode ser fornecido em appliance físico, desde que homologado pelo fabricante da solução;

21.4.1.3. Pode ser fornecido em formato de software ou imagem ISO de instalação, compatível com VMWare nas versões ESXi 6.5.0 ou 6.7.0 em processadores Intel;

21.4.1.4. Deve suportar máquinas virtuais com Sistema Operacional Windows 7 ou superior.

21.4.2. Características

21.4.2.1. Ser do mesmo fabricante e integrado com a solução de proteção de estações de trabalho;

21.4.2.2. Suportar atualização da base de dados, integrado à Rede de Inteligência do fabricante, de forma automática e sem causar nenhum tipo de indisponibilidade da solução;

21.4.2.3. A análise inicial deve ser realizada de forma local no ambiente de detecção, o envio de artefatos para verificação na Sandbox deve ocorrer de forma automática, ou seja, caso a inteligência do produto identifique a necessidade de encaminhar o objeto para análise na Sandbox, este processo deve ocorrer sem a intervenção do usuário;

21.4.2.4. Permitir arquitetura em Cluster, possibilitando o compartilhamento de informações entre servidores;

21.4.2.5. Um único servidor deve ter a capacidade mínima de processar objetos recebidos de:

21.4.2.6. Estações de trabalho, ou;

21.4.2.7. Sistemas externos usando API.

21.4.2.8. O agente do Sandbox deve ser gerenciado através da mesma console da solução;

21.4.2.9. Permitir o armazenamento de arquivos de rastreamento e logs do sistema, contendo os seguintes itens:

21.4.2.10. Nomes dos arquivos enviados para verificação;

21.4.2.11. Informar Endereços IP e nomes de hosts que enviaram arquivos para análise em Sandbox;

21.4.2.12. Endereços IP e nomes dos servidores Sandbox que estão no mesmo cluster;

21.4.2.13. Nome da conta de administrador do servidor Sandbox;

21.4.2.14. Endereço IP e nome do servidor proxy;

21.4.2.15. Endereço IP e nome do servidor de gerenciamento;

21.4.2.16. Endereços IP e nomes de servidores de atualização.

21.4.2.17. Permitir que os dados dos eventos sejam armazenados e disponibilizem, no mínimo as seguintes informações:

21.4.2.18. Usuário da sessão no Sistema Operacional;

21.4.2.19. Contas de usuários no Sistema Operacional;

21.4.2.20. Erros da execução de tarefas de escaneamento dos objetos;

21.4.2.21. Tarefas de escaneamento de objetos;

21.4.2.22. Detecções;

21.4.2.23. Resultado do escaneamento de objetos;

21.4.2.24. Objetos que estão em fila para envio ao Sandbox;

21.4.2.25. Modificações realizadas no agente do Sandbox e políticas da console de gerenciamento;

21.4.2.26. Objetos quarentenados;

21.4.2.27. Permitir o gerenciamento do Sandbox por meio de interface Web;

21.4.2.28. Permitir integração de sistemas terceiros através de interface REST API;

21.4.2.29. No caso de oferta local, ter acesso à console do servidor do Sandbox através de acesso SSH ou por terminal;

21.4.2.30. Permitir tomar ações em um objeto que tente coletar atividades da internet por meio da interface de rede do servidor de Sandbox;

21.4.2.31. Deve suportar a análise dos seguintes formatos de arquivos:

21.4.2.32. PDF;

21.4.2.33. Portable Executable (PE).

21.4.2.34. Deve suportar a análise dos seguintes formatos Microsoft Office:

21.4.2.35. DOC, DOCX, PPSX, XLS, XLSX, PPT, PPTX.

21.5. Detecção e Resposta

21.5.1. Características

21.5.1.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na console integrada da solução de proteção de estações de trabalho;

21.5.1.2. A solução deve oferecer módulo focado em capacidades de EDR "Endpoint Detection and Response", incluindo no mínimo as seguintes capacidades:

21.5.1.3. O agente deve ter capacidade de coletar e processar dados relacionadas ao veredito e ao contexto da ameaça;

21.5.1.4. Deve fornecer graficamente a visualização da cadeia do ataque;

21.5.1.5. Deve possuir a capacidade de varredura, para identificar a presença de um artefato detectado em outros dispositivos na rede, através de indicadores de comprometimento (IoC).

21.5.1.6. A varredura deve oferecer opções de resposta automatizada (sem intervenção do administrador), para serem executadas caso o IoC seja encontrado em outro dispositivo, com no mínimo as seguintes opções:

21.5.1.7. Isolar o host;

21.5.1.8. Iniciar uma varredura nas áreas críticas;

21.5.1.9. Quarentenar o objeto;

21.5.1.10. Capacidade de integração com a solução de sandbox;

21.5.1.11. A solução deve disponibilizar informações detalhadas sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

21.5.1.12. Detecções provenientes da solução de endpoint;

21.5.1.13. Detecções provenientes da solução de sandbox;

21.5.1.14. Processos;

21.5.1.15. Alterações de registro;

21.5.1.16. DLL's

21.5.1.17. Conexões remotas;

21.5.1.18. Criação de arquivos;

21.5.1.19. Varredura por todos os dispositivos executada a partir de indicador de comprometimento (IoC) gerado através da solução e importado pelo administrador.

21.5.1.20. Possibilidade de exportar os indicadores de comprometimento (IoC).

21.5.1.21. A solução deve oferecer no mínimo as seguintes opções de resposta:

21.5.1.22. Prevenir a execução de um arquivo;

21.5.1.23. Quarentenar um arquivo;

21.5.1.24. Iniciar uma varredura por IoC;

21.5.1.25. Parar um processo;

21.5.1.26. Ferramenta que possibilite o isolamento do host infectado com no mínimo as características abaixo:

21.5.1.27. A opção de isolamento deve estar disponível junto a visualização do incidente;

21.5.1.28. Na configuração padrão, o isolamento deve ser feito de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra.

22. ITEM 2 - SOLUÇÃO DE SEGURANÇA DE ENDPOINT (DESKTOPS), COM XDR E SANDBOX

22.1. Requisitos Gerais

22.1.1. Prover segurança para as estações de trabalho (endpoints), sejam físicas ou em ambiente virtualizado;

22.1.2. Se comunicar com a Gerência Integrada da solução, de forma que seja possível gerenciar todas as funcionalidades;

22.1.3. Detectar e eliminar programas maliciosos (malwares), tais como vírus, ransomware, spywares, worms, cavalos de tróia, keyloggers, programas de propaganda, rootkits, phishing, dentre outros;

22.1.4. Identificar e proteger contra eventuais vulnerabilidades dos sistemas operacionais e aplicações;

22.1.5. Deve detectar e eliminar programas maliciosos em:

22.1.5.1. Processos em Execução em memória principal (RAM);

22.1.5.2. Arquivos executados, criados, copiados, renomeados, movidos ou modificados, inclusive em sessões de linha de comando (DOS ou Shell);

22.1.5.3. Arquivos compactados, em tempo real ou no ato de sua execução, com os seguintes formatos: ZIP, EXE, ARJ, RAR, e CAB;

22.1.5.4. Detectar e proteger em tempo real a estação de trabalho contra vulnerabilidades e ações maliciosas executadas em navegadores web por meio de scripts em linguagens tais como javascript, vbscript/Activex.

22.1.6. Capacidade de detecção heurística de malwares desconhecidos;

22.1.7. Possuir tecnologia de Machine Learning de pre−execution, run time machine e post−execution;

22.1.8. Deve prover, no mínimo, as seguintes proteções:

22.1.8.1. Antivírus de arquivos;

22.1.8.2. Antivírus web (verificação de sites e downloads contra malwares);

22.1.8.3. Firewall de host com HIPS (Host Intrusion Prevention System) e/ou HIDS (Host Intrusion Detection System);

22.1.8.4. Proteção contra ataques aos serviços/processos do antivírus;

22.1.8.5. Controle de dispositivos;

22.1.8.6. Controle de execução de arquivo e aplicativos também por meio hash;

22.1.8.7. Bloqueio de sites maliciosos categorizados de acordo com a nuvem do fabricante;

22.1.8.8. Prevenção contra exploração de vulnerabilidades.

22.1.8.9. Capacidade de integração com a Antimalware Scan Interface (AMSI);

22.1.8.10. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

22.1.8.11. Controle de vulnerabilidades do Windows e de softwares de terceiros instalados;

22.1.8.12. Capacidade de bloquear as vulnerabilidades de forma automática e informar o CVE, quando relacionado, de acordo com a severidade;

22.1.8.13. Capacidade de gerenciar as políticas de bloqueio de vulnerabilidades, fazendo o deploy das regras de acordo com as características do dispositivo.

22.2. Detalhamento das proteções:

22.2.1. Antivírus de arquivos:

22.2.1.1. Verificar todos os arquivos criados, acessados ou modificados, inclusive em sessões de linha de comando (DOS ou shell) abertas pelo usuário;

22.2.1.2. Deve possuir módulo que analise as ações de cada aplicação em execução no computador, gravando as ações executadas e comparando−as com sequências características de atividades perigosas. Tais registros de sequências devem ser atualizados juntamente com as vacinas;

22.2.1.3. Deve possuir Módulo que analise cada macro de VBA executada, procurando por sinais de atividade maliciosa;

22.2.1.4. Deve possuir módulo que analise qualquer tentativa maliciosa de edição, exclusão ou gravação do registro;

22.2.1.5. Capacidade para definir escopo de varredura/rastreamento de todos os discos locais e em discos específicos;

22.2.1.6. Capacidade de adicionar pastas/arquivos em uma zona de exclusão, a fim de excluí-los da verificação;

22.2.1.7. Possibilidade de definir frequência de varredura;

22.2.1.8. Capacidade de realizar a verificação "inteligente" de arquivos, ou seja, somente verificará o arquivo se este for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomá−la apenas a partir da extensão do arquivo;

22.2.1.9. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto.

22.2.2. Antivírus web:

22.2.2.1. Possuir módulo de web-antivírus para proteção contra ameaças durante navegação na internet;

22.2.2.2. Capacidade de limitar o acesso a sites da internet por reputação;

22.2.2.3. Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus web;

22.2.2.4. Capacidade de verificar tráfego nos browsers: Internet Explorer, Mozilla Firefox e Google Chrome.

22.2.3. Firewall de host com HIPS e/ou HIDS

22.2.3.1. O módulo de firewall deve conter, no mínimo, dois conjuntos de regras:

22.2.3.2. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas ou, definir o comportamento da filtragem de pacotes, podendo definir pelo menos, mas não limitado a: permitir, bloquear ou bloquear com exceções aos pacotes de rede;

22.2.3.3. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo terá acesso à rede;

22.2.3.4. Deve possuir módulo HIPS e/ou HIDS para proteção/detecção contra port scans e exploração de vulnerabilidades de softwares. A base de dados de análise deve ser atualizada juntamente com as vacinas.

22.2.3.5. A solução deve permitir a análise comportamental avançada de aplicativos e arquivos executáveis com indícios maliciosos (Ransomware);

22.2.3.6. A solução deve ser capaz de avaliar aplicações desconhecidas e potencialmente maliciosas permitindo sua execução e analisando seu comportamento no endpoint;

22.2.3.7. Deve permitir criar exceções para aplicações confiáveis, evitando que sejam bloqueadas por componentes de detecção;

22.2.3.8. Não deve requerer conexão com centro de inteligência do fabricante para que a proteção seja ativada ou executada;

22.2.3.9. A Solução deve manter um cache de reputação local com informações de aplicações conhecidas, desconhecidas e maliciosas;

22.2.3.10. Dentre os comportamentos maliciosos, deve ser capaz de "bloquear" ou "detectar e trazer rastreabilidade sobre":

22.2.3.11. Acesso local a partir de cookies;

22.2.3.12. Criação de arquivos a partir de arquivos com extensão .bat, .exe, html, hpg, bmp, job e .vbs;

22.2.3.13. Criação de threads em outro processo;

22.2.3.14. Desativação de executáveis críticos do sistema operacional;

22.2.3.15. Leitura/Exclusão/Gravação de arquivos visados por Ransomwares;

22.2.3.16. Gravação e Leitura na memória de outro processo;

22.2.3.17. Modificação da política de firewall do Windows;

22.2.3.18. Modificação da pasta de tarefas do Windows;

22.2.3.19. Modificação de arquivos críticos do Windows e Locais do Registro;

22.2.3.20. Modificação de arquivos executáveis portáteis;

22.2.3.21. Modificação de bit de atributo oculto;

22.2.3.22. Modificação de bit de atributo somente leitura;

22.2.3.23. Modificação de entradas de registro de DLL AppInit;

22.2.3.24. Modificação de locais do registro de inicialização;

22.2.3.25. Modificação de pastas de dados de usuários;

22.2.3.26. Modificação do local do Registro de Serviços;

22.2.3.27. Suspensão de um processo.

22.2.3.28. Deve ser capaz de bloquear ou apenas informar quando uma ameaça for encontrada;

22.2.3.29. Deve ser capaz de informar ao usuário as ameaças encontradas através de mensagem;

22.2.3.30. Deve possuir modo de ativação da análise comportamental avançada para quaisquer arquivos desconhecidos acessados pelo sistema operacional e nunca antes visto pela solução;

22.2.3.31. Deve ser possível atribuir a regra conforme política equilibrada, visando maior segurança ou produtividade do usuário;

22.2.3.32. A proteção deve estar contida no mesmo agente de proteção, não requerendo outro software ou aplicação adicional na estação de trabalho para a execução e ativação da proteção;

22.2.3.33. Utilizar técnicas de machine learning para detecção de ameaças;

22.2.3.34. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning).

22.2.4. Criptografia

22.2.4.1. O acesso ao recurso criptografado (arquivo, pasta ou disco) deve ser garantido mesmo em caso o usuário tenha esquecido a senha, através de procedimentos de recuperação;

22.2.4.2. Deve ser compatível com sistemas operacionais para estações de trabalho Windows;

22.2.4.3. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;

22.2.4.4. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;

22.2.4.5. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;

22.2.4.6. Permitir criar vários usuários de autenticação pré-boot;

22.2.4.7. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;

22.2.4.8. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;

22.2.4.9. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:

22.2.4.10. Criptografar somente os arquivos novos que forem copiados para o disco removível, sem modificar os arquivos já existentes;

22.2.4.11. Criptografar todos os arquivos individualmente;

22.2.4.12. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;

22.2.4.13. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;

22.2.4.14. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente.

22.2.4.15. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;

22.2.4.16. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;

22.2.4.17. Verificar compatibilidade de hardware antes de aplicar a criptografia;

22.2.4.18. Possibilitar estabelecer parâmetros para a senha de criptografia;

22.2.4.19. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;

22.2.4.20. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo

22.2.4.21. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;

22.2.4.22. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;

22.2.4.23. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de áudio;

22.2.4.24. Permite criar um grupo de extensõ es de arquivos a serem criptografados;

22.2.4.25. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;

22.2.4.26. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento;

22.2.4.27. Capacidade de deletar arquivos de forma segura após a criptografia;

22.2.4.28. Capacidade de criptografar somente o espaço em disco utilizado;

22.2.4.29. Deve ter a opção de criptografar arquivos criados a partir de aplicação es selecionadas pelo administrador;

22.2.4.30. Permitir criptografia de dispositivos móveis (Notebooks) quando o endpoint não possuir comunicação com a console de gerenciamento;

22.2.4.31. Capacidade de bloquear aplicação es selecionadas pelo administrador de acessarem arquivos criptografados;

22.2.4.32. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo;

22.2.4.33. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;

22.2.4.34. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;

22.2.4.35. Capacidade de fazer "Hardware encryption";

22.2.5. Controle de dispositivos:

22.2.5.1. Deve possuir módulo de controle de dispositivos, que permita o bloqueio e a ativação de dispositivos, no mínimo as seguintes categorias:

22.2.5.2. Discos de armazenamento locais;

22.2.5.3. Armazenamento removível;

22.2.5.4. Impressoras;

22.2.5.5. CD/DVD;

22.2.5.6. Drives de disquete;

22.2.5.7. Modems;

22.2.5.8. Dispositivos multifuncionais;

22.2.5.9. Leitores de smart card;

22.2.5.10. Dispositivos de sincronização via ActiveSync (Windows CE, Windows Mobile);

22.2.5.11. Wi-Fi;

22.2.5.12. Adaptadores de rede externos;

22.2.5.13. Dispositivos MP3 ou smartphones;

22.2.5.14. Dispositivos Bluetooth;

22.2.5.15. Câmeras e Scanners.

22.2.5.16. Capacidade de liberar o acesso a um dispositivo específico sem a necessidade de desabilitar a proteção ou da intervenção local na máquina do usuário;

22.2.5.17. Capacidade de adicionar novos dispositivos por Class ID/Hardware ID.

22.2.6. Controle de execução de aplicativos:

22.2.6.1. O módulo de controle de aplicações deve prover a capacidade de visibilidade sobre as aplicações executadas e aplicar o controle de execução imposto pela política;

22.2.6.2. Deve ser capaz de realizar um inventário das estações de trabalho protegidas informando todos os executáveis presentes;

22.2.6.3. Como resultado da varredura, a solução deve armazenar o nome completo da aplicação, checksum, nome da aplicação ou versão da aplicação e fabricante;

22.2.6.4. Informação completa de hardware contendo: processadores, memória, adaptadores de vídeo, discos de armazenamento, adaptadores de áudio, adaptadores de rede, monitores, drives de CD/DVD;

22.2.6.5. Ao detectar uma aplicação, deverá consultar a solução de reputação de arquivos e compartilhamento de informações de segurança;

22.2.6.6. Caso não seja possível efetuar comunicação com a Solução de reputação de arquivos e compartilhamento de informações de segurança, o módulo deve realizar consulta de reputação para o Centro de Inteligência do fabricante;

22.2.6.7. Deve ser possível criar uma imagem base para a criação de uma política geral;

22.2.6.8. Capacidade de trabalhar no modo adaptativo, ou seja, adaptando−se à novas aplicações instaladas na máquina;

22.2.6.9. Deve identificar as aplicações de maneira única através do uso de hash (MD5 ou SHA− 1);

22.2.6.10. A solução deve suportar as seguintes modalidades de proteção:

22.2.6.11. Criação de uma lista de aplicações autorizadas que podem ser executadas, onde todas as demais aplicações são impedidas de serem executadas;

22.2.6.12. Criação de uma lista de aplicações não autorizadas que não podem ser executadas;

22.2.6.13. Monitoração e proteção de aplicativos e componentes críticos do sistema operacional de serem adulterados em tempo de execução, isto é, durante operação e execução em memória.

22.2.6.14. Deve ser capaz de proteger em modo standalone − online ou offline;

22.2.6.15. Além de possuir um conjunto de regras, deve permitir por parte do administrador que este customize−as de forma a adaptar a necessidade do órgão;

22.2.6.16. Permitir o bloqueio de aplicações e os processos que a aplicação interage;

22.2.6.17. Permitir monitoração de aplicações onde se pode determinar quais processos poderão ser executados ou não;

22.2.6.18. Permitir monitoração de Hooking de aplicações;

22.2.7. Proteção contra ransomwares:

22.2.7.1. Bloquear a criptografia de arquivos em recursos compartilhados a partir de um processo malicioso, inclusive, que esteja sendo executado em outra máquina;

22.2.7.2. Monitoramento de pastas compartilhadas no ambiente Windows, rastreando o estado dos arquivos armazenados e os protegendo;

22.2.7.3. Na detecção de atividade maliciosa de criptografia por ransomware, o antivírus deve interromper o processo de criptografia e restaurar os arquivos ao seu estado original, impedindo a perda de dados corporativos.

22.2.8. Compatibilidade

22.2.8.1. O software de proteção deve ser compatível com as seguintes versões de sistemas operacionais Windows para estações de trabalho:

22.2.8.2. Microsoft Windows 8.1 (e suas edições);

22.2.8.3. Microsoft Windows 10 (e suas edições);

22.2.8.4. Ser compatível para instalação em sistemas legados em Windows 7 (e suas edições).

22.2.8.5. O software de proteção deve ser compatível com as seguintes versões de sistemas operacionais Windows para servidores:

22.2.8.6. Microsoft Windows Server 2008 R2 (e suas edições);

22.2.8.7. Microsoft Windows Server 2012 (e suas edições);

22.2.8.8. Microsoft Windows Server 2012 R2 (e suas edições);

22.2.8.9. Microsoft Windows Server 2016 (e suas edições);

22.2.8.10. Microsoft Windows Server 2019 (e suas edições).

22.2.9. Para desktop Mac OS X

22.2.10. Compatibilidade:

22.2.11. macOS Mojave 10.14

22.2.12. macOS Catalina 10.15

22.2.13. macOS Big Sur 11.0

22.2.14. Características:

22.2.14.1. Deve prover proteção residente para arquivos (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;

22.2.14.2. Possuir módulo de web-antivírus para proteção contra ameaças durante navegação na internet;

22.2.14.3. Possuir módulo de bloqueio a ataques na rede;

22.2.14.4. Possibilidade de bloquear ameaças entre a máquina atacante e os demais computadores, durante o ataque;

22.2.14.5. Capacidade de criar exclusão para computadores em relação a varreduras;

22.2.14.6. Possibilidade de importar uma chave no pacote de instalação;

22.2.14.7. Capacidade de escolher de quais módulos serão instalados;

22.2.14.8. As vacinas devem ser atualizadas, no mínimo uma vez por dia pelo fabricante e disponibilizada aos usuários independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

22.2.14.9. Capacidade de voltar para a base de dados de vacina anterior;

22.2.14.10. Capacidade de criar alertas de ataques por e-mail;

22.2.14.11. Capacidade de adicionar pastas para uma zona de exclusão, a fim de excluí-las da verificação. Capacidade, também, de adicionar arquivos à lista de exclusão;

22.2.14.12. Possibilidade de pausar automaticamente varreduras agendadas quando o computador estiver consumindo alto recurso de CPU;

22.2.14.13. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

22.2.14.14. Capacidade de verificar somente arquivos novos e alterados;

22.2.14.15. Capacidade de verificar objetos usando heurística;

22.2.14.16. Capacidade de agendar uma pausa na verificação;

22.2.14.17. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

22.2.14.18. Perguntar o que fazer, ou;

22.2.14.19. Bloquear acesso ao objeto;

22.2.14.20. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

22.2.14.21. Caso positivo de desinfecção:

22.2.14.22. Restaurar o objeto para uso;

22.2.14.23. Caso negativo de desinfecção:

22.2.14.24. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

22.2.14.25. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

22.2.14.26. Capacidade de verificar arquivos de formato de e-mail;

22.2.14.27. Possibilidade de trabalhar com o produto pela linha de comando, com no mínimo opções para atualizar as vacinas, iniciar uma varredura, para o antivírus e iniciar o antivírus pela linha de comando;

22.2.14.28. Capacidade de, através da console de gerência integrada;

22.2.14.29. Ser instalado;

22.2.14.30. Ser removido;

22.2.14.31. Ser gerenciado;

22.2.15. Estações de trabalho Linux

22.2.16. Compatibilidade:

22.2.17. Plataforma 64-bits:

22.2.17.1. Red Hat Enterprise Linux 6.7 e superior;

22.2.17.2. Ubuntu 16.04 LTS e superior;

22.2.17.3. CentOS 6.7 e superior;

22.2.17.4. Debian GNU / Linux 8.6 e superior;

22.2.17.5. Oracle Linux 7.3 e superior;

22.2.17.6. SUSE Linux Enterprise Server 15 e superior.

22.2.18. Características:

22.2.19. Deve prover as seguintes proteções:

22.2.19.1. Antivírus de arquivos residente, tais como: anti-spyware, anti-trojan, anti-malware, que verifique qualquer arquivo criado, acessado ou modificado;

22.2.19.2. Deve permitir gerenciamento, no mínimo, das seguintes formas:

22.2.19.3. Via linha de comando;

22.2.19.4. Via console administrativa;

22.2.19.5. Via GUI;

22.2.19.6. Via web (remotamente).

22.2.19.7. Deve possuir funcionalidade de scan de drives removíveis para, no mínimo:

22.2.19.8. Flash drives (pen drives);

22.2.19.9. HDs externos;

22.2.19.10. Deve fornecer varredura em compartilhamentos e unidades de rede mapeadas:

22.2.19.11. Por arquivos;

22.2.19.12. Por pastas/diretórios.

22.2.19.13. As vacinas devem ser atualizada, no mínimo, uma vez por dia pelo fabricante;

22.2.19.14. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

22.2.19.15. Capacidade de criar exclusões por local, máscara e nome da ameaça;

22.2.19.16. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

22.2.19.17. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

22.2.19.18. Fazer detecções através de heurística;

22.2.19.19. Gerenciamento de Quarentena: Quarentena de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de quarentena;

22.2.19.20. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.

22.2.19.21. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

22.2.19.22. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;

22.2.19.23. Capacidade de verificar objetos usando heurística;

22.2.19.24. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

22.2.19.25. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

22.2.19.26. Detecção de phishing e sites maliciosos;

22.2.19.27. Bloqueio de download de arquivos maliciosos;

22.2.19.28. Bloqueio de adware;

22.2.19.29. Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

22.2.19.30. Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).

22.2.19.31. Deve possuir módulo de proteção contra criptografia maliciosa.

22.2.20. XDR Detecção e Resposta para desktop Linux e Windows;

22.2.21. A funcionalidade de EDR e cliente de antivírus devem ser integradas, sendo possível instalar mais de um componente para a proteção do desktop, caso necessário;

22.2.22. A ferramenta de EDR deve fazer detecção através do comportamento;

22.2.23. Deve fazer o correlacionamento de eventos entre computadores na rede (IoC Scanning);

22.2.24. Deve detectar elevação de privilégio;

22.2.25. Deve enviar objetos para verificação no Sandbox de forma automática quando necessário utilizando a inteligência global da fabricante;

22.2.26. Deve enviar objetos para verificação em Sandbox de forma manual;

22.2.27. O EDR deve permitir coletar informações forenses do endpoint tais como:

22.2.27.1. Dados;

22.2.27.2. Dumps de memória;

22.2.27.3. Estado do sistema operacional;

22.2.27.4. Processos iniciados;

22.2.27.5. Conexões estabelecidas;

22.2.27.6. Arquivos criados;

22.2.27.7. Registro modificado;

22.2.27.8. Tentativas de conexão com um host remoto;

22.2.27.9. Tentativa de login com sucesso;

22.2.27.10. Tentativa de login com falha;

22.2.28. Para segurança da comunicação entre o EDR e a Console de Gerência integrada deve utilizar certificado ou token;

22.2.29. O EDR deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades abaixo:

22.2.29.1. Parar um processo;

22.2.29.2. Deletar um objeto;

22.2.29.3. Quarentenar um arquivo;

22.2.29.4. Recuperar um arquivo;

22.2.29.5. Prevenir a execução de um arquivo;

22.2.29.6. Executar um script;

22.2.29.7. Isolar o host completamente e de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

22.2.30. Deve ser possível realizar a customização de indicador de ataques IoA;

22.2.31. Deve ter capacidade de apresentar informações relacionadas ao MITRE ATT&CK para cada um dos eventos detectados no ambiente, caso possuam;

22.2.32. Deverá possuir modulo de pesquisa para descoberta de ameaças (Threat Hunting);

22.2.33. Deverá possuir acesso ao portal de inteligência de ameaças da própria fabricante;

22.2.34. No portal deverá ser possível buscar informações sobre indicadores de ataques, consultas de domínios na base global de ameaças do próprio fabricante.

22.2.35. Possuir funcionalidade integrada de emulação para malware, onde as ameaças sejam analisadas em sandbox, em ambiente controlado, em nuvem própria do fabricante ou em ambiente computacional da Justiça Eleitoral.

22.2.36. Deverá realizar emulação em sandbox nos seguintes sistemas operacionais:

22.2.36.1. Windows 7, 64-bit.

22.2.36.2. Windows 10, 64-bit.

22.2.37. Deverá ser possível prevenir ataques de forma automatizada baseada na resposta da sandbox.

23. ITEM 3 - SOLUÇÃO DE SEGURANÇA PARA SERVIDORES (LINUX E WINDOWS), COM XDR E SANDBOX

23.1. SERVIDORES LINUX

23.1.1. Compatibilidade:

23.1.1.1. Plataforma 64-bits:

23.1.1.2. Red Hat Enterprise Linux 6.7 e superior;

23.1.1.3. Ubuntu 16.04 LTS e superior;

23.1.1.4. CentOS 6.7 e superior;

23.1.1.5. Debian GNU / Linux 8.6 e superior;

23.1.1.6. Oracle Linux 7.3 e superior;

23.1.1.7. SUSE Linux Enterprise Server 15 e superior.

23.1.2. Características da solução de proteção:

23.1.2.1. Deve prover as seguintes proteções:

23.1.2.2. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;

23.1.2.3. Deve ser capaz detectar vírus, worms, trojans, toolkits, adware, auto-dialers e outros tipos de ameaças;

23.1.2.4. Deve possuir módulo de proteção baseado em comportamento;

23.1.2.5. Deve possuir funcionalidade para identificar as aplicações maliciosas ou não nos servidores com opção de bloquear ou permitir;

23.1.2.6. Deve ter a capacidade de criar regras para controle de uma aplicação utilizando hash ou nome da aplicação.

23.1.2.7. Ter a capacidade de detectar e aplicar as regras necessárias nos módulos e políticas de varredura para cada servidor, de forma automática, ou pelo administrador;

23.1.2.8. Deve permitir gerenciamento, no mínimo, das seguintes formas:

23.1.2.9. Via linha de comando;

23.1.2.10. Via console administrativa;

23.1.2.11. Via GUI;

23.1.2.12. Via web;

23.1.2.13. Deve possuir funcionalidade de scan de drives removíveis para, no mínimo:

23.1.2.14. Flash drives;

23.1.2.15. HDs externos;

23.1.2.16. Deve fornecer varredura em compartilhamentos e unidades de rede mapeadas:

23.1.2.17. Por arquivos;

23.1.2.18. Por pastas/diretórios.

23.1.2.19. As vacinas devem ser atualizadas, no mínimo, uma vez por dia pelo fabricante;

23.1.2.20. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

23.1.2.21. Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfectar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;

23.1.2.22. Gerenciamento de Quarentena: Deve bloquear objetos suspeitos;

23.1.2.23. Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados);

23.1.2.24. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;

23.1.2.25. Capacidade de customizar o uso de memória ou processamento em varreduras agendadas;

23.1.2.26. Capacidade de verificar objetos usando heurística;

23.1.2.27. Possibilidade da solução realizar backup dos arquivos infectados antes de realizar uma ação;

23.1.2.28. Fazer detecções através de heurística.

23.1.2.29. O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:

23.1.2.30. Detecção de phishing e sites maliciosos;

23.1.2.31. Bloqueio de download de arquivos maliciosos;

23.1.2.32. Bloqueio de adware.

23.1.2.33. Deve possuir módulo de proteção contra criptografia maliciosa, protegendo contra tentativas de criptografia remota;

23.1.2.34. Deve possuir recurso contra ataques maliciosos;

23.1.2.35. Deve possuir recurso para restabelecimento de arquivos contra ataques maliciosos.

23.1.2.36. Deve realizar busca de vírus e malwares em ambientes Docker e Contâiner;

23.1.2.37. Deverá ser considerado proteção para contâiner em, no máximo, 30 (trinta) servidores físicos. Este item é exclusivo para atendimento ao ambiente do Tribunal Superior Eleitoral.

23.1.3. SERVIDORES WINDOWS

23.1.4. Compatibilidade:

23.1.4.1. Microsoft Windows Server 2019 Essentials / Standard / Datacenter;

23.1.4.2. Microsoft Windows Server 2016 Essentials / Standard / Datacenter;

23.1.4.3. Microsoft Windows Server 2012 R2 Foundation / Essentials / Standard / Datacenter;

23.1.4.4. Microsoft Windows Server 2012 Foundation / Essentials / Standard / Datacenter;

23.1.4.5. Microsoft Windows Server 2008 R2 Foundation / Essentials / Standard / Datacenter SP1;

23.1.4.6. Deve suportar as seguintes plataformas virtualizadas:

23.1.4.7. VMware Workstation 16 Pro;

23.1.4.8. VMware ESXI 7.0. e superior;

23.1.4.9. Microsoft Hyper-V Server 2019;

23.1.4.10. Citrix Hypervisor 8.2 LTSR;

23.1.5. Características da solução de proteção:

23.1.5.1. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware) que verifique qualquer arquivo criado, acessado ou modificado;

23.1.5.2. Auto-proteção contra-ataques aos serviços/processos do antivírus;

23.1.5.3. Firewall com IDS;

23.1.5.4. Controle de vulnerabilidades do Windows e dos aplicativos instalados;

23.1.5.5. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;

23.1.5.6. Deve permitir gerenciamento, no mínimo, das seguintes formas:

23.1.5.7. Via console administrativa;

23.1.5.8. Via web (remotamente);

23.1.5.9. As vacinas devem ser atualizadas, no mínimo, uma vez por dia pelo fabricante;

23.1.5.10. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:

23.1.5.11. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);

23.1.5.12. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

23.1.5.13. Leitura de configurações;

23.1.5.14. Modificação de configurações;

23.1.5.15. Gerenciamento de Backup e Quarentena;

23.1.5.16. Visualização de logs;

23.1.5.17. Gerenciamento de logs;

23.1.5.18. Gerenciamento de ativação da aplicação;

23.1.5.19. Gerenciamento de permissões (adicionar/excluir permissões acima);

23.1.5.20. Deve possuir bloqueio de inicialização de aplicativos baseado em white lists.

23.1.5.21. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

23.1.5.22. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

23.1.5.23. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

23.1.5.24. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

23.1.5.25. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede;

23.1.5.26. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros);

23.1.5.27. Em caso de erros, deve ter capacidade de criar logs e traces automaticamente, sem necessidade de outros softwares;

23.1.5.28. Deve possuir funcionalidade de análise personalizada de logs do Windows;

23.1.5.29. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

23.1.5.30. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

23.1.5.31. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

23.1.5.32. Capacidade de adicionar pastas para uma zona de exclusão, a fim de excluí-las da verificação. Capacidade, também, de adicionar arquivos à lista de exclusão;

23.1.5.33. Capacidade de verificar arquivos por conteúdo, ou seja, somente verificará o arquivo se for passível de infecção. O antivírus deve analisar a informação de cabeçalho do arquivo para fazer essa decisão e não tomar a partir da extensão do arquivo;

23.1.5.34. Capacidade de verificar somente arquivos novos e alterados;

23.1.5.35. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários);

23.1.5.36. Capacidade de verificar objetos usando heurística;

23.1.5.37. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

23.1.5.38. Capacidade de agendar uma pausa na verificação;

23.1.5.39. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:

23.1.5.40. Perguntar o que fazer, ou;

23.1.5.41. Bloquear acesso ao objeto;

23.1.5.42. Apagar o objeto ou tentar desinfectá-lo (de acordo com a configuração pré-estabelecida pelo administrador);

23.1.5.43. Caso positivo de desinfecção:

23.1.5.44. Restaurar o objeto para uso;

23.1.5.45. Caso negativo de desinfecção:

23.1.5.46. Mover para quarentena ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

23.1.5.47. Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;

23.1.5.48. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em quarentena;

23.1.5.49. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

23.1.5.50. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:

23.1.5.51. Executar os procedimentos pré-configurados pelo administrador;

23.1.5.52. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

23.1.5.53. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

23.1.5.54. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros;

23.1.5.55. Capacidade de detectar anomalias no comportamento de um software, usando análise heurística e aprendizado de máquina (machine learning);

23.1.5.56. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

23.1.6. XDR para servidores (EDR Extendido)

23.1.6.1. A funcionalidade de EDR e cliente de antivírus devem ser integradas sendo configurado pela mesma gerência;

23.1.6.2. A ferramenta de EDR deve fazer detecção através do comportamento;

23.1.6.3. Deve fazer o correlacionamento de eventos entre computadores na rede (IoC Scanning);

23.1.6.4. Deve detectar elevação de privilégio;

23.1.6.5. Deve enviar objetos para verificação em Sandbox de formar manual e automática;

23.1.6.6. O EDR deve permitir coletar informações forenses do endpoint tais como:

23.1.6.7. Dados;

23.1.6.8. Dumps de memória;

23.1.6.9. Estado do sistema operacional;

23.1.6.10. Processos iniciados;

23.1.6.11. Conexões estabelecidas;

23.1.6.12. Arquivos criados;

23.1.6.13. Registro modificado;

23.1.6.14. Tentativas de conexão com um host remoto;

23.1.6.15. Tentativa de login com sucesso;

23.1.6.16. Tentativa de login com falha.

23.1.6.17. Para segurança entre a comunicação entre o EDR e a Console de gerenciamento um certificado deve ser utilizado;

23.1.6.18. O EDR deve ser capaz de executar tarefas para todo o ambiente e para dispositivos específicos, contendo no mínimo as capacidades abaixo:

23.1.6.19. Parar um processo;

23.1.6.20. Deletar um objeto;

23.1.6.21. Quarentenar um arquivo;

23.1.6.22. Recuperar um arquivo;

23.1.6.23. Prevenir a execução de um arquivo;

23.1.6.24. Executar um script;

23.1.6.25. Isolar o host completamente e de forma granular, permitindo o controle do dispositivo pela console administrativa mesmo após ativação da regra;

23.1.6.26. Deve ser possível realizar a customização de indicador de ataques IoA;

23.1.6.27. Deve ter capacidade de apresentar informações relacionadas ao MITRE ATT&CK para cada um dos eventos detectados no ambiente, caso possuam;

23.1.6.28. Deverá possuir modulo de pesquisa para descoberta de ameaças (Threat Hunting);

23.1.6.29. Deverá possuir acesso ao portal de inteligência de ameaças da própria fabricante.

23.1.6.30. No portal deverá ser possível buscar informações sobre indicadores de ataques, consultas de domínios na base global de ameaças do próprio fabricante;

23.1.6.31. Possuir funcionalidade integrada de emulação para malware, onde as ameaças sejam analisadas em Sandbox, em ambiente controlado, em nuvem própria do fabricante ou em ambiente computacional da Justiça eleitoral;

23.1.6.32. Deverá realizar emulação em Sandbox nos seguintes sistemas operacionais:

23.1.6.33. Windows 7, 64-bit;

23.1.6.34. Windows 10, 64-bit;

23.1.6.35. Deverá ser possível prevenir ataques de forma automatizada baseada na resposta da Sandbox;

24. ITEM 4 - SERVIÇOS DE INSTALAÇÃO, CONFIGURAÇÃO E IMPLANTAÇÃO DA SOLUÇÃO (PARCELA ÚNICA):

24.1. A CONTRATADA será inteiramente responsável pela instalação da solução antivírus atualmente em uso pelo CONTRATANTE, bem como pelas despesas diretas ou indiretas para execução das atividades pela sua equipe técnica;

24.2. A instalação dos softwares em estações de trabalho, conforme limite estabelecido no item 24.3.2, podendo ser realizada remotamente, por meio de ferramenta a ser acordada com o Contratante;

24.3. A instalação das consoles de gerência da solução será realizada remotamente em 28 (vinte e oito) sítios distintos, conforme abaixo:

24.3.1. 01 (uma) no Tribunal Superior Eleitoral e 27 (vinte e sete) localizadas nos Tribunais Regionais Eleitorais, sendo uma instalação em cada regional;

24.3.2. Deverá ser realizada a instalação dos softwares em 10 (dez) estações de trabalho e 5 (cinco) servidores de cada sítio, remotamente;

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

24.5. A instalação da solução deverá ser realizada em horário de expediente de cada sítio, podendo ocorrer no período de 8h às 20hs;

24.6. O processo de instalação e configuração da solução deverá ser acompanhado por servidores do TSE ou dos TRE, de acordo com a sua localidade;

24.7. Para garantir que a instalação não afete o ambiente do CONTRATANTE, os procedimentos e atividades deverão ser realizados por técnicos certificados pelo fabricante;

24.8. A CONTRATADA deverá se reunir com a equipe técnica do CONTRATANTE, por solicitação desta, e elaborar um plano de migração, em até 10 (dez) dias úteis, contendo as etapas, modelos, arquiteturas, funcionalidades e configurações da solução que serão implantadas durante a execução do serviço de migração;

24.9. Caso alguma instalação mostre-se não funcional ou apresente problemas, será feita a comunicação do CONTRATANTE para a CONTRATADA, por e-mail ou abertura de chamado. A instalação deverá ser refeita em até 2 (dois) dias úteis a contar da comunicação feita pelo CONTRATANTE.

25. ITEM 5 - QUANTO A TRANSFERÊNCIA DE CONHECIMENTO:

25.1. A transferência de conhecimento será solicitada por e-mail, ao critério da CONTRATANTE, com um prazo igual ou maior que 15 dias para iniciá-la.

25.1.1. A transferência de conhecimento deverá ser realizada de forma remota e no prazo máximo de até 90 (noventa) dias, contados da assinatura do Contrato.

25.2. A CONTRATADA deverá realizar a transferência de conhecimento para a equipe técnica do CONTRATANTE, por meio de treinamento oficial nas tecnologias da solução, com carga horária total de 40 (quarenta) horas.

25.3. A carga horária diária será de 4h (quatro horas). O treinamento deverá ocorrer em dias úteis e em horário comercial.

25.4. A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizada nas dependências do Tribunal Superior Eleitoral, conforme decisão do CONTRATANTE.

25.5. Cada turma referente a transferência de conhecimentos será compostas de: no mínimo 15 (quinze) e no máximo 25 (vinte e cinco) alunos.

25.6. A transferência de conhecimento deverá conter conteúdo teórico e prático e deverá abordar, no mínimo, os seguintes itens:

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

25.6.2. Orientar sobre os componentes, procedimentos de instalação e administração da solução unificada de segurança para endpoint e EDR, explorando todas as funcionalidades exigidas na especificação técnica.

25.6.3. Orientar sobre a topologia lógica da solução implantada, mostrando a interligação dos componentes físicos e virtuais da solução, informando as interconexões realizadas com a infraestrutura existente no CONTRATANTE.

25.6.4. 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.

25.7. O cronograma efetivo da transferência de conhecimento será definido em conjunto com o CONTRATANTE, após a solicitação realizada por e-mail, no prazo de 7 dias corridos.

25.8. Caso o CONTRATANTE solicite alterações no programa de transferência de conhecimento, a CONTRATADA terá até 2 (dois) dias corridos para apresentação de uma nova versão do programa. Eventuais mudanças de conteúdo solicitadas pelo CONTRATANTE deverão constar no material didático. O CONTRATANTE terá até 2 (dois) dias úteis para aprovação da nova versão do programa.

25.9. Deverá ser disponibilizado material didático em formato digital, sem custo adicional para o CONTRATANTE. Todo material deverá estar, preferencialmente, em língua portuguesa (Brasil), podendo ser em idioma estrangeiro (inglês).

25.10. Deverá ser emitido certificado de participação ao final do curso a cada participante, detalhando programa e carga horária.

25.11. A CONTRATADA deverá aplicar um questionário de avaliação para preenchimento obrigatório de todos os servidores treinados, previamente acordado com a fiscalização do contrato. Será considerado como satisfatório o percentual de aprovação acima de 70% (setenta por cento).

25.11.1. O questionário de avaliação será aplicado na última hora da transferência de conhecimento.

25.12. Caso a transferência de conhecimento não seja satisfatória em relação aos aspectos relacionados à carga horária, programa apresentado e estrutura, esta deverá ser realizada novamente, sem ônus adicional ao CONTRATANTE.

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

ANEXO I-II - MODELO DE PROPOSTA

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

Tabela - Licitação por Lote

Lote	Item	Descrição*	Unidade de Medida	Quantidade	Valor Unitário (Anual) Por solução/Serviços	Valor Unitário (60 meses) Por solução/Serviços	Valor Glo (Por 60 me
1	1	Solução de segurança de EndPoint (**desktops**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	35.906			
	2	Solução de Segurança de EndPoint (**desktops**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	21.077			
	3	Solução de Segurança para Servidores (**Linux e Windows**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	8.360			
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).	Unidade	28			
	5	Transferência de conhecimento (parcela única).	Unidade	4 turmas			
						Valor Total - Lote 1 (R$)	

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

Declarações:
i) Esta empresa declara que tem pleno conhecimento das condições necessárias para o fornecimento/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 i
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 Edi
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
1,2 e 3	As subscrições entregas correspondem ao objeto contratado?			
1,2 e 3	As subscrições foram entregues no prazo estipulado?			
4	Os serviços de instalação foram realizados dentro do prazo previsto?			
4	Os serviços de instalação foram realizados nas quantidades previstas no contrato?			
5	A transferência de conhecimento foi realizada em até 15 dias da sua solicitação?			
5	A carga horária foi cumprida?			
5	O questionário de avaliação atingiu o percentual de aprovação acima de 70% (setenta por cento)?			

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 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 TSE nº:
Objeto:
Vigência:

Fiscalização: Memorando nº (SEI nº)
Fiscal Técnico Titular:
Fiscal Técnico Substituto:

ITEM	CRITÉRIO DE CONFERÊNCIA	SIM	NÃO
1	**ASPECTOS QUANTITATIVOS:**		
1.1	A quantidade de subscrições é igual à definida no contrato?		
1.2	Cada tipo de licença foi entregue com funcionalidade plena e respectiva documentação exigida em contrato?		
	Os serviços de instalação foram realizados nas quantidades previstas no contrato?		
2	**ASPECTOS QUALITATIVOS**:		
2.1	Todos os itens possuem mesma marca e modelo (versão) do cotado?		
2.2	Todos os itens possuem especificações compatíveis com o Edital e correspondentes à proposta da licitante vencedora?		
2.3	Todos os softwares estão registrados em nome do Contratante?		
2.4	O questionário de avaliação da transferência de conhecimento atingiu o percentual de aprovação acima de 70% (setenta por cento)?		
3	**OUTRAS OBRIGAÇÕES CONTRATUAIS**:		
3.1	Em caso de reprovação de itens os problemas foram sanados em no máximo 7 (sete) dias úteis após a notificação?		
3.2	A Contratada realizou a instalação e configuração dentro do prazo contratado?		
3.3	Os serviços de suporte e garantia foram prestados conforme as exigências contratuais?		

	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, qualita
obrigações contratuais, a fiscalização decide por:

	RECEBER DEFINITIVAMENTE O OBJETO
	NÃO RECEBER DEFINITIVAMENTE O OBJETO

ANEXO I-IV - 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 repres
Representante, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Rep**
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 Co**
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 se

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 quai situações emergenciais de pronto atendimento.
d)	Agilizar os contatos com os representantes da administração durante a execução do contrato.
e)	Atender aos empregados em serviço, nas dependências do Contratante, com a entrega de documentos pertinentes, uniformes, equipam outros necessários à boa execução contratual.
f)	Manter a ordem, a disciplina e o respeito, junto a todo o pessoal da Contratada, orientando e instruindo os empregados quanto à fo proporcionar ambiente de trabalho harmonioso.
g)	Observar, orientar e fiscalizar os profissionais quanto ao horário de trabalho; ao correto uso dos uniformes, equipamentos de proteção e apresentação compatível, promovendo, junto à respectiva Contratada, a correção das falhas verificadas.
h)	Providenciar junto à Contratada as aplicações de advertências, suspensões ou devoluções de profissionais que não cumprirem com suas obrigaç de insubordinação, indisciplina ou desrespeito.
i)	Desenvolver outras atividades de responsabilidade da Contratada, principalmente quanto ao controle de informações relativas ao seu contra 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 **(DD**
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 c
Superior Eleitoral.

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 - QUANTIDADE MÍNIMA

Tabela - Licitação por Lote				
Lote	**Item**	**Descrição***	**Unidade de Medida**	**Quantidade**
1	1	Solução de segurança de EndPoint (**desktops**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	14.000
	2	Solução de Segurança de EndPoint (**desktops**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	100
	3	Solução de Segurança para Servidores (**Linux e Windows)**, com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	Unidade	100
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).	Unidade	1
	5	Transferência de conhecimento (parcela única).	Unidade	1 turma

ANEXO I-VII - QUANTIDADES ESTIMADA PELOS TREs E TSE

TRIBUNAL	ITEM 1	ITEM 2	ITEM 3	ITEM 4	ITEM 5
TRE - AC	-	226	128	-	-
TRE - AL	-	-	120	-	-
TRE - AM	-	-	-	-	-
TRE - AP	-	350	100	-	-
TRE - BA	-	1627	200	-	-
TRE - CE	-	500	1.000	-	-
TRE - DF	-	1.000	350	-	-
TRE - ES	-	1.050	160	-	-
TRE - GO	-	1.000	300	-	-
TRE - MA	-	-	250	-	-
TRE - MG	-	5.500	315	-	-
TRE - MS	-	-	-	-	-
TRE - MT	-	378	185	-	-
TRE - PA	-	1.800	260	-	-
TRE - PB	-	150	200	-	-
TRE - PE	-	-	100	-	-
TRE - PI	-	200	220	-	-
TRE - PR	-	2.500	500	-	-
TRE - RJ	-	720	262	-	-
TRE - RN	-	-	190	-	-
TRE - RO	-	280	160	-	-
TRE - RR	-	200	125	-	-
TRE - RS	-	500	230	-	-
TRE - SC	-	100	250	-	-
TRE - SE	-	760	126	-	-
TRE - SP	-	-	250	-	-
TRE - TO	-	-	280	-	-
TSE	35.906	2.236	2.099	28	4
TOTAL REGISTRADO	**35.906**	**21.077**	**8.360**	**28**	**4**

ADAÍRES AGUIAR LIMA
SECRETÁRIO(A) DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **29/11/2021, às 21:01**, 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=1855955&crc=411651DA, informando, caso não preenchido, o código verificador **1855955** e o código CRC **411651DA**.

Brasília/DF, 15 de dezembro de 2021.

AO
TRIBUNAL SUPERIOR ELEITORAL - TSE
A/C: Comissão Permanente de Licitação

Ref.: PROPOSTA COMERCIAL – PREGÃO ELETRÔNICO Nº 84/2021
Processo: 2021.00.000003531-9

Prezada Sr(a). Pregoeiro(a),

Apresentamos, a seguir, Proposta Comercial para Registro de preços para contratação de subscrições de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento, com pagamento anual, pelo período de 60 meses, consoante especificações, exigências e prazos constantes deste Termo de Referência, em atendimento às necessidades do Tribunal Superior Eleitoral (TSE).

Após cuidadoso exame e estudo do Edital de Licitação em referência, seus Anexos e os Esclarecimentos divulgados, com os quais estamos de pleno acordo para atendimento integral, vimos apresentar nossa Proposta de Preços para contratação de empresas especializada para atendimento das demandas da Secretaria de Tecnologia da Informação (STI), de acordo com as especificações técnicas e quantidades constantes no Edital do Pregão Eletrônico.

Quaisquer tributos, custos e despesas diretos ou indiretos omitidos da Proposta ou incorretamente cotados serão considerados como inclusos nos preços, não sendo considerados, em caso de adjudicação, pleitos de acréscimos, a esse ou qualquer título, isentando o TSE de quaisquer ônus adicionais. Declaramos que nos preços propostos estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto desta Licitação.

A apresentação da Proposta Comercial implica na plena aceitação do cumprimento das condições estabelecidas no Edital e seus Anexos, assumindo a DFTI o compromisso de executar os serviços nos seus termos, bem como de fornecer os softwares, materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

Declaramos que todos os prazos estabelecidos no Termo de Referência e seus Anexos serão cumpridos e nos responsabilizamos pelas transações efetuadas em nosso nome, assumindo como firmes e verdadeiras nossas propostas e lances, inclusive os atos praticados diretamente ou por nosso representante, não cabendo ao TSE responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros, e temos pleno conhecimento dos termos do edital e seus anexos.

A empresa DFTI Comércio e Serviços de Informática LTDA declara o pleno atendimento aos requisitos técnicos e habilitatórios e que a proposta apresentada está em conformidade com as exigências contidas no referido Edital e em seus anexos.

Declaramos pleno conhecimento das condições necessárias para o fornecimento/prestação dos serviços.

Obrigamo-nos, caso nos seja adjudicado o objeto do Pregão em causa, a celebrar a assinatura do Contrato.

1. SOLUÇÃO OFERTADA

1.1. Para atendimento à demanda de Solução de segurança de EndPoint (desktops) e Servidores (Linux e Windows), com EDR/XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, ofertamos os produtos do fabricante Trend Micro.

1.2. Mais informações no site do fabricante Trend Micro: http://www.trendmicro.com.br/

2. DOS SERVIÇOS

2.1. Suporte Técnico

Os serviços de Suporte Técnico apresentados serão na modalidade “24x5”, e a cada abertura de incidente será aberta uma OS com o tempo limite para atendimento conforme SLA para início das atividades da equipe de suporte DFTI (remoto ou on-site), dependendo da criticidade e solicitação por parte do cliente. Para a presente proposta, apresentamos a seguir um breve descritivo das modalidades de atendimento a incidentes e problemas com a solução ofertada, bem como os seus procedimentos de abertura:

A. Solicitação de Abertura de Chamado e Suporte Telefônico

O primeiro nível de atendimento deverá ser iniciado através dos números: **(61) 3024-8411** ou **0800 601 DFTI** (3384), para registro dos chamados de suporte e início dos atendimentos.

B. Solicitação de Abertura de Chamado e Suporte via e-mail

Através do e-mail suporte@dfti.com.br poderão ser inseridas todas as informações, de forma detalhada, sobre os problemas encontrados na solução ofertada.

C. Suporte On-site

Caso se faça necessário, e após a conclusão inicial dos atendimentos de suporte (itens A e B acima) o suporte técnico poderá ser escalado para o atendimento presencial (On-site), em Brasília, a ser prestado por técnico qualificado e certificado nos produtos sob garantia e suporte.

2.2. Treinamento

O treinamento, sob demanda, onde cada turma referente a transferência de conhecimentos será composta de: no mínimo 15 (quinze) e no máximo 25 (vinte e cinco) alunos, em atendimento a todas as exigências descritas no Edital e seus anexos.

A carga horária diária será de 4h (quatro horas). O treinamento deverá ocorrer em dias úteis e em horário comercial.

A transferência de conhecimento deverá ser realizada de forma remota ou poderá ser realizada nas dependências do Tribunal Superior Eleitoral, mediante anuência do mesmo.

3. CONDIÇÕES COMERCIAIS

Tabela - Licitação por Lote							
	Item	**Descrição***	**Unidade de Medida**	**Quantidade**	**Valor Unitário (Anual) Por solução/Serviços**	**Valor Unitário (60 meses) Por solução/Serviços**	**Valor Global (Por 60 meses)**
Lote	1	Solução de segurança de EndPoint (desktops), com EDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + EDR/XDR: Endpoint and Server + Deep Discovery Analyzer	Unidade	35.906	R$ 39,40	R$ 197,00	R$ 7.073.482,00
	2	Solução de Segurança de EndPoint (desktops), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + Deep Security System + XDR: Endpoint and Server + Deep Discovery Analyzer	Unidade	21.077	R$ 39,40	R$ 197,00	R$ 4.152.169,00

	3	Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses. Marca: TRENDMICRO Modelos: Trend Micro Smart Protection for Endpoints + Deep Security System + XDR: Endpoint and Server + Deep Discovery Analyzer	Unidade	8.360	R$ 46,00	R$ 230,00	R$ 1.922.800,00
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).	Unidade	28	R$ 3.000,00 (Valor unitário)	R$ 3.000,00 (Valor unitário)	R$ 84.000,00
	5	Transferência de conhecimento (parcela única).	Unidade	4	R$ 8.000,00 (Valor por turma)	R$ 8.000,00 (Valor por turma)	R$ 32.000,00
						Valor Total - Lote 1 (R$)	**R$ 13.264.451,00**

4. CONDIÇÕES GERAIS

Validade da proposta: 60 (sessenta) dias.
Prazo de entrega: Conforme Edital e seus Anexos.
Pagamento: Conforme Edital e Seus Anexos.
Garantia dos produtos e Serviços: Serviços de Suporte Técnico, com manutenção, garantia (update e upgrade) por 60 (sessenta) meses, conforme exigido no Edital e seus Anexos
Obs: Declaramos o pleno atendimento a todos os itens exigidos no edital e seus anexos para fins de inclusão em nossa proposta.

5. INFORMAÇÕES CADASTRAIS

RAZÃO SOCIAL	DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA
NOME FANTASIA	DFTI - TECNOLOGIA DA INFORMAÇÃO
ENDEREÇO	SCN Qd. 02 Bloco D - Torre A - Nº 810 Liberty Mall, Brasília/DF, CEP: 70.712-903
CNPJ	09.650.283/0001-91
INSC. ESTADUAL	07.505.692/001-81
TELEFONE / FAX	(61) 3030-1000
EMAIL	dfti@dfti.com.br
WEBSITE	www.dfti.com.br
DADOS BANCÁRIOS	[redacted]

Demais condições conforme Edital do Pregão Eletrônico nº 84/2021 e seus anexos.

Colocamo-nos à sua inteira disposição para dirimir eventuais dúvidas relacionadas ao teor da presente proposta bem como às especificações dos produtos e serviços apresentados.

Atenciosamente,

FABRICIO BOMBARDA GUEDES:[redacted]
Digitally signed by FABRICIO BOMBARDA GUEDES:[redacted]

Fabrício Bombarda
Diretor Executivo e Representante Legal
CPF: 819.649.861-68
RG: 1.563.949 SSP/DF
Tel.: (61) 3030-1000
Cel.: (61) 99291-7070
fabricio@dfti.com.br

PREGÃO ELETRÔNICO

PODER JUDICIÁRIO
Tribunal Superior Eleitoral

Termo de Homologação do Pregão Eletrônico
Nº 00084/2021 (SRP)

Às 16:22 horas do dia 28 de dezembro de 2021, após constatada a regularidade dos atos procedimentais, a autoridade competente, Sr. RUI MOREIRA DE OLIVEIRA, HOMOLOGA a adjudicação referente ao Processo nº 202100000003531-9, Pregão nº 00084/2021.

Resultado da Homologação

Grupo 1
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Critério de Valor: R$ 24.359.440,0600
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 13.264.451,0000 .

Itens do grupo:

- 1 - Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
- 2 - Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
- 3 - Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
- 4 - Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
- 5 - Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador

Item: 1 - Grupo 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: Solução de segurança de EndPoint (desktops dos ambientes dos 27 TREs), com EDR e Sandbox , com manutenção, garantia (update e upgrade) e suporte por 60 meses, com pagamento de subscrições a cada 12 meses.
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 35.906 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 281,9500 **Intervalo Mínimo entre Lances:** -
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 197,0000 **e a quantidade de** 35.906 **UNIDADE** .

Eventos do Item

Evento	Data	Nome	Observações
Adjudicado	21/12/2021 16:00:39	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:00:48	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:00:54	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:01:01	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:01:09	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$

			197,0000
Adjudicado	21/12/2021 16:01:16	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Homologado	28/12/2021 16:22:44	RUI MOREIRA DE OLIVEIRA	

Item: 2 - Grupo 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: Soluça~o de Segurança de EndPoint (desktops), com XDR e Sandbox, com manutença~o, garantia (update e upgrade) por 60 meses, com pagamento de subscriço~es a cada 12 meses
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 21.077 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 415,0000 **Intervalo Mínimo entre Lances:** -
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 197,0000 **e a quantidade de** 21.077 **UNIDADE** .

Eventos do Item

Evento	Data	Nome	Observações
Adjudicado	21/12/2021 16:00:41	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:00:49	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:00:55	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:01:02	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:01:10	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Adjudicado	21/12/2021 16:01:17	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 197,0000
Homologado	28/12/2021 16:22:47	RUI MOREIRA DE OLIVEIRA	

Item: 3 - Grupo 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: Solução de Segurança para Servidores (Linux e Windows), com XDR e Sandbox, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 8.360 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 605,0000 **Intervalo Mínimo entre Lances:** -
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 230,0000 **e a quantidade de** 8.360 **UNIDADE** .

Eventos do Item

Evento	Data	Nome	Observações
Adjudicado	21/12/2021 16:00:42	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000
Adjudicado	21/12/2021 16:00:50	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000
Adjudicado	21/12/2021 16:00:56	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000

Adjudicado	21/12/2021 16:01:03	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000
Adjudicado	21/12/2021 16:01:11	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000
Adjudicado	21/12/2021 16:01:18	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 230,0000
Homologado	28/12/2021 16:22:50	RUI MOREIRA DE OLIVEIRA	

Item: 4 - Grupo 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 28 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 12.213,8700 **Intervalo Mínimo entre Lances:** -
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 3.000,0000 **e a quantidade de** 28 **UNIDADE** .

Eventos do Item

Evento	Data	Nome	Observações
Adjudicado	21/12/2021 16:00:43	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Adjudicado	21/12/2021 16:00:52	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Adjudicado	21/12/2021 16:00:58	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Adjudicado	21/12/2021 16:01:04	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Adjudicado	21/12/2021 16:01:12	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Adjudicado	21/12/2021 16:01:19	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 3.000,0000
Homologado	28/12/2021 16:22:53	RUI MOREIRA DE OLIVEIRA	

Item: 5 - Grupo 1
Descrição: Licenciamento de Direitos Permanentes de Uso de Outros Softwares / Programas de Computador
Descrição Complementar: Transferência de conhecimento (parcela única).
Tratamento Diferenciado: -
Aplicabilidade Margem de Preferência: Não
Quantidade: 4 **Unidade de fornecimento:** UNIDADE
Valor Máximo Aceitável: R$ 22.250,0000 **Intervalo Mínimo entre Lances:** -
Situação: Homologado

Adjudicado para: DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA **, pelo melhor lance de** R$ 8.000,0000 **e a quantidade de** 4 **UNIDADE** .

Eventos do Item

Evento	Data	Nome	Observações
Adjudicado	21/12/2021 16:00:44	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 8.000,0000
Adjudicado	21/12/2021 16:00:53	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$

			8.000,0000
Adjudicado	21/12/2021 16:00:59	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 8.000,0000
Adjudicado	21/12/2021 16:01:06	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 8.000,0000
Adjudicado	21/12/2021 16:01:14	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 8.000,0000
Adjudicado	21/12/2021 16:01:20	-	Adjudicação individual da proposta. Fornecedor:DFTI - COMERCIO E SERVICOS DE INFORMATICA LTDA, CNPJ/CPF:09.650.283/0001-91, Melhor lance : R$ 8.000,0000
Homologado	28/12/2021 16:22:56	RUI MOREIRA DE OLIVEIRA	

Fim do documento

TRIBUNAL SUPERIOR ELEITORAL

ATA DE REGISTRO DE PREÇOS TSE Nº 1/2022

EVENTUAL CONTRATAÇÃO DE SUBSCRIÇÕES DE SOLUÇÃO DE ANTIVÍRUS COM EDR
2021.00.000003531-9

Aos 4 (quatro) dias do mês de janeiro do ano de 2022, o Tribunal Superior Eleitoral, com sede no Setor de Administração Federal Sul, SAFS Q. 7, Lotes 1 e 2, Brasília/DF, CNPJ nº 00.509.018/0001-13, neste ato representado pela **DIRETORA-GERAL DA SECRETARIA SUBSTITUTA**, Senhora **ADAÍRES AGUIAR LIMA**, portadora da Carteira de Identidade n° 2973335 SSP/DF, inscrita no CPF sob o n° 316.257.972-49, no uso de suas atribuições legais, resolve, nos termos das Leis nº 8.666/93 e nº 10.520/2002 e pelo Decreto nº 7.892/2013, em face da **Licitação TSE nº 84/2021**, PA SEI nº 2021.00.000003531-9, modalidade pregão, forma eletrônica – SRP, registrar os preços da **DFTI - COMÉRCIO E SERVIÇOS DE INFORMÁTICA LTDA.**, segundo as seguintes cláusulas e condições:

1. DO OBJETO

A presente ata tem por objeto o registro de preços para eventual contratação de subscrições de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento, com pagamento anual, pelo período de 60 (sessenta) meses, consoante especificações, condições, quantidades e prazos constantes do Termo de Referência - Anexo I do Edital.

Farão parte deste Registro de Preços, como órgãos participantes, os Tribunais Regionais Eleitorais – TREs, que serão responsáveis pelas suas respectivas contratações.

2. DA EMPRESA REGISTRADA

Empresa **DFTI - Comércio e Serviços de Informática Ltda.,** CNPJ nº 09.650.283/0001-91, com sede SCN Quadra 02, Bloco D, Torre A, nº 810 - Liberty Mall - Brasília/DF. CEP. 70.712-903. Fone: (61) 3030-1000 ou (61) 99291-7070. E-mail: fabricio@dfti.com.br; representado por seu Representante Legal, Senhor **Fabrício Bombarda Guedes**, RG nº 1.563.949 SSP/DF e CPF 819.649.861-68.

3. DOS PREÇOS REGISTRADOS

3.1. Os preços, as quantidades e as especificações dos produtos/serviços registrados constam da proposta da empresa adjudicatária e do Anexo II-I - Itens Registrados, desta Ata de Registro de Preços.

4. DA ASSINATURA DO TERMO DE CONTRATO E DO PEDIDO DE FORNECIMENTO DOS PRODUTOS/PRESTAÇÃO DE SERVIÇOS

4.1 Após a assinatura desta ata de registro de preços, sempre que houver necessidade de fornecimento dos produtos/prestação de serviços, o TSE/TRE convocará a empresa cujo preço foi registrado para assinatura do termo de contrato correspondente, de acordo com as especificações constantes do Termo de Referência - Anexo I do Edital da Licitação.

4.1.1. A contratada deverá entregar as subscrições no prazo máximo de 30 (trinta) dias corridos e contados do início da vigência do contrato. As licenças deverão ser entregues em formato digital, para o e-mail SESAP@tse.jus.br, ou para download em site do fabricante do produto.

4.1.2. A contratada deverá concluir a instalação de todos os 28 (vinte e oito) sítios, a configuração e a ativação das subscrições em até 35 (trintas) dias após o início da vigência contratual.

4.1.3. A contratada deverá providenciar a renovação das subscrições nos 30 (trinta) dias que antecederem o vencimento das mesmas, com validade à partir do vencimento das subscrições ativas.

4.1.3.1. As subscrições renovadas devem ser entregues e ativadas, no máximo, até o vencimento das subscrições em uso de modo a não haver interrupção nos serviços.

4.1.4. Os Tribunais Regionais Eleitorais farão suas contratações em apartado, na condição de partícipes da Ata de Registro de Preços.

4.2. A empresa convocada fica obrigada a atender todos os pedidos efetuados durante a validade desta ata de registro de preços.

4.3. Ao assinar a ata de registro de preços, a contratada obriga-se a fornecer os produtos/prestar os serviços conforme especificações e condições contidas no Edital de Licitação TSE nº 84/2021 e seus anexos e na proposta apresentada, prevalecendo, no caso de divergência, as especificações e condições do edital.

4.4. Quando a contratada não aceitar a nota de empenho ou instrumento equivalente, sem justificativa, seu registro será cancelado nos termos do art. 20, II, do Decreto nº 7.892/2013, sem prejuízo das penalidades cabíveis. Nesse caso, serão convocadas as demais empresas registradas no cadastro de reserva, na ordem de classificação, conforme o disposto no art. 11, inciso IV, daquele Decreto.

4.5. A regra é a contratação por lote. A Administração somente poderá contratar cada item que compõe o lote de forma independente, se tiver obtido o menor preço nos lances individuais por item, para aquele item pretendido.

5. DAS OBRIGAÇÕES DAS PARTES

5.1 Constituem obrigações do TSE (órgão gerenciador), além das especificadas no Edital de Licitação TSE nº 84/2021 e seus anexos:

5.1.1. gerenciar a ata de registro de preços, providenciando a indicação, sempre que solicitado, da empresa registrada, para atendimento às necessidades da Administração, obedecendo os quantitativos definidos no Edital de Licitação TSE nº 84/2021;

5.1.2. notificar a contratada de qualquer irregularidade encontrada na execução do objeto;

5.1.2.1. Esta obrigação compete também aos Tribunais Regionais Eleitorais participantes deste Registro de Preços em relação às suas contratações.

5.1.3. promover ampla pesquisa de mercado, de forma a comprovar que os preços registrados permanecem compatíveis com os praticados;

5.1.4. conduzir os procedimentos relativos a eventuais negociações dos preços registrados e à aplicação de penalidades por descumprimento do pactuado nesta Ata de Registro de Preços ou das obrigações contratuais, em relação às suas próprias contratações.

5.2. Constituem obrigações da empresa registrada, além das discriminadas no Edital de Licitação TSE nº 84/2021:

5.2.1. assinar esta ata e aceitar a respectiva nota de empenho, conforme previsto;

5.2.2. fornecer, sempre que solicitado, no prazo máximo de 5 (cinco) dias úteis, a contar da notificação, documentação de habilitação e qualificação cujas validades encontrem-se vencidas;

5.2.3. manter atualizados os dados da empresa e de seus representantes, tais como: endereços, telefones, e-mail, dentre outros.

6. DA LIQUIDAÇÃO E DO PAGAMENTO

6.1. O pagamento será efetuado após o recebimento definitivo, até o 10º (décimo) dia útil, a partir do atesto da 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, cumpridos os requisitos dispostos no Capítulo XIII do Edital de Licitação TSE nº 84/2021.

6.2. Os Tribunais Regionais Eleitorais participantes deste Registro de Preços se responsabilizarão pelo pagamento à contratada pelo fornecimento dos produtos/prestação dos serviços de acordo com o quantitativo adquirido por cada um deles.

7. DA ATUALIZAÇÃO MONETÁRIA

Nos casos de pagamento efetuados após 30 (trinta) dias da emissão do Termo de Recebimento Definitivo ou da apresentação da nota fiscal, conforme o caso, desde que a contratada não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo TSE, entre o 31º (trigésimo primeiro) dia e a data da emissão da ordem bancária, será a seguinte:

EM = I x N x VP

Onde:

EM = encargos moratórios;

N = número de dias entre a data prevista para o pagamento e a do efetivo pagamento;

VP = valor da parcela a ser paga;

I = 0,0001644 (índice de compensação financeira por dia de atraso, assim apurado: I = (6/100)/365).

8. DAS ALTERAÇÕES DA ATA DE REGISTRO DE PREÇOS

8.1. Esta ata de registro de preços poderá sofrer alterações, obedecidas as disposições contidas nos artigos 17, 18 e 19 do Decreto n.° 7.892/2013.

8.2. O preço registrado poderá ser revisto em decorrência de eventual redução daqueles praticados no mercado, ou de fato que eleve o custo do objeto registrado, cabendo ao TSE promover as necessárias negociações com a empresa registrada, observadas as disposições contidas na alínea "d", inciso II do art. 65 da Lei n.º 8.666/93.

8.3. Quando o preço inicialmente registrado, por motivo superveniente, tornar-se superior ao praticado no mercado, o TSE deverá convocar a empresa registrada visando a negociação para redução de preços e sua adequação ao praticado pelo mercado, podendo liberá-la do compromisso assumido, se frustrada a negociação.

8.4. Quando o preço de mercado tornar-se superior aos preços registrados e a empresa registrada, mediante requerimento devidamente comprovado, não puder cumprir o compromisso, o TSE poderá liberá-la do compromisso assumido, caso a comunicação ocorra antes do pedido de execução do objeto e sem aplicação da penalidade, confirmando a veracidade dos motivos e comprovantes apresentados.

8.5. Não havendo êxito na negociação, o TSE deverá proceder à revogação da ata de registro de preços, adotando as medidas cabíveis para obtenção da contratação mais vantajosa.

9. DA REVOGAÇÃO DA ATA E DO CANCELAMENTO DO REGISTRO

9.1. O inadimplemento de condições estabelecidas nesta ata de registro de preços, por parte da empresa registrada, assegurará ao TSE o direito de revogar o respectivo registro do fornecedor inadimplente, mediante notificação, com prova de recebimento;

9.2. A empresa registrada terá seu registro cancelado quando:

a) descumprir as condições desta ata de registro de preços;

b) não aceitar a respectiva nota de empenho ou instrumento equivalente, no prazo estabelecido pela Administração, sem justificativa aceitável;

c) não aceitar reduzir o seu preço registrado, na hipótese de este se tornar superior àqueles praticados no mercado;

d) sofrer sanção prevista nos incisos III ou IV do art. 87 da Lei n.° 8.666/93 ou no art. 7° da Lei n.° 10.520/2002.

9.3. O cancelamento de registro do fornecedor, nas hipóteses previstas nas alíneas "a", "b" e "d", assegurados o contraditório e a ampla defesa, será formalizado por despacho da autoridade competente do TSE.

9.4. O cancelamento do registro de preço poderá ocorrer por fato superveniente que venha comprometer a perfeita execução contratual, decorrentes de caso fortuito ou força maior, devidamente comprovados:

a) por razão de interesse público; ou

b) a pedido da licitante registrada.

9.5. Além das hipóteses previstas no item 9.2 acima, constituem ainda motivos para o cancelamento do registro do respectivo fornecedor:

a) atraso injustificado na prestação dos serviços, bem como a sua paralisação sem justa causa e prévia comunicação ao TSE;

b) cometimento reiterado de falhas comprovadas por meio de registro próprio efetuado pela fiscalização;

c) transferir a outrem, no todo ou em parte, o objeto registrado;

9.6. Na ocorrência do cancelamento do registro de um fornecedor, nas situações descritas nos arts. 20 e 21 do Decreto nº 7.892/2013, serão convocadas as demais empresas registradas no cadastro de reserva, na ordem de classificação, conforme o disposto no art. 11, IV, §§ 1º, 2º e 3º do Decreto nº 7.892/2013.

10. DA VIGÊNCIA

A vigência desta ata de registro de preços é de 1 (um) ano, contado da publicação do seu extrato no órgão da Imprensa Oficial.

11. DAS PENALIDADES

A empresa registrada ficará sujeita, assim como as integrantes dos cadastro de reserva, que convocadas, não honrarem o compromisso assumido sem justificativa aceita pela Administração, nos casos de inexecução total ou parcial de suas obrigações, às sanções previstas no Capítulo XIV do Edital de Licitação do TSE n.° 84/2021, assegurados o contraditório e a ampla defesa, sem prejuízo do ressarcimento dos danos porventura causados à Administração.

12. DAS DISPOSIÇÕES GERAIS

12.1. A existência de preços registrados não obriga a Administração a contratar, facultando-se a realização de licitação específica para a contratação pretendida, assegurada preferência à licitante registrada em igualdade de condições.

12.2. A empresa registrada nesta ata declara estar ciente de suas obrigações para com o TSE, nos termos do Edital de Licitação TSE nº 84/2021 e da sua proposta, que passam a fazer parte da presente ata e a reger as relações entre as partes, para todos os fins.

12.3. Cabe ao órgão participante, garantida a ampla defesa e o contraditório, aplicar as penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preços ou do descumprimento das obrigações contratuais, em relação às suas próprias contratações, informando as ocorrências ao TSE (órgão gerenciador).

12.4. Será permitida aos Tribunais Regionais Eleitorais não participantes a adesão à Ata de Registro de Preços proveniente deste Pregão para aquisição dos itens 2 e 3 do Termo de Referência - Anexo I deste Edital.

12.4.1. O quantitativo decorrente das adesões à ata de registro de preços para os Tribunais Regionais Eleitorais não participantes, não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata para o TSE (órgão gerenciador) e para os TREs participantes, independente do número de TREs não participantes que aderirem.

12.4.2. Não será permitida a adesão de nenhum órgão não participante da ata e não pertencente à Justiça Eleitoral.

12.5. As demais condições estão consignadas nos seguintes documentos, que são parte desta ata, independentemente de transcrição:

12.5.1. Edital de Licitação TSE nº 84/2021.

12.5.2. Termo de Referência, correspondente ao Anexo I do Edital da Licitação TSE nº 84/2021.

12.5.3. Proposta da empresa registrada, ajustada ao último lance do pregão.

12.5.4. Ata de realização da sessão pública do pregão, que conterá a informação das licitantes que aceitaram reduzir seus preços aos da licitante vencedora, para efeito de cadastro de reserva.

13. DO FORO

O foro da Seção Judiciária do Distrito Federal é o competente para solucionar conflitos de interesses entre o TSE e a empresa registrada relativos à presente ata.

14. DA PUBLICIDADE

O extrato da presente ata de registro de preços será publicado no órgão da imprensa oficial, conforme o disposto no parágrafo único do art. 61 da Lei nº 8.666/93.

ANEXO II-I - ITENS REGISTRADOS - ATA DE REGISTRO DE PREÇOS TSE Nº 84/2021

No dia 04 de janeiro de 2022, no Tribunal Superior Eleitoral, órgão gerenciador desta Ata, registram-se os preços da empresa abaixo identificada para contratação de solução de antivírus com EDR para estações e servidores, serviço de instalação e transferência de conhecimento conforme descrito no quadro abaixo, resultante do Pregão Eletrônico TSE nº 84/2021. As especificações técnicas constantes do Procedimento Administrativo nº 2021.00.000003531-9, bem assim a Proposta de Preços integram esta Ata de Registro de Preços, independente de transcrição.

Esta ata de registro de preços tem vigência de um ano, **até ___ de _____ de 2022.**

Lote	Item	Descrição	Qtd.	Valor Unitário Registrado
1	1	Solução de segurança de EndPoint (**desktops**), com **EDR e Sandbox** , com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	35.906	R$ 197,00
	2	Solução de Segurança de EndPoint (**desktops**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	21.077	R$ 197,00
	3	Solução de Segurança para Servidores (**Linux e Windows**), com **XDR e Sandbox**, com manutenção, garantia (update e upgrade) por 60 meses, com pagamento de subscrições a cada 12 meses.	8.360	R$ 230,00
	4	Serviços de instalação, configuração, implantação da solução + repasse de conhecimento hands-on (parcela única).	28	R$ 3.000,00
	5	Transferência de conhecimento (parcela única).	4	R$ 8.000,00

E por estarem assim, justas e acordadas, as partes assinam o presente anexo em duas vias de igual teor e forma para todos os fins de direito.

Pelo órgão gerenciador:

Adaíres Aguiar Lima
Diretora-Geral de Secretaria do TSE - Substituta

Pela empresa registrada:

Fabrício Bombarda Guedes
Representante Legal da empresa

FABRICIO BOMBARDA GUEDES
USUÁRIO EXTERNO

Documento assinado eletronicamente em **04/01/2022, às 18:52**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

ADAÍRES AGUIAR LIMA
DIRETORA-GERAL - SUBSTITUTA

Documento assinado eletronicamente em **07/01/2022, às 14:16**, 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=1893282&crc=B7BF59F0, informando, caso não preenchido, o código verificador **1893282** e o código CRC **B7BF59F0**.