TRIBUNAL SUPERIOR ELEITORAL

ANEXO I DO EDITAL - TERMO DE REFERÊNCIA

PREGÃO ELETRÔNICO TSE Nº 90032/2024

1. OBJETO

1.1. Registro de preço para eventual aquisição de subscrições para solução de proteção DNS, suporte, garantia e serviços de planejamento e configuração, consoante especificações, exigências, quantidades e prazos constantes deste Termo de Referência.

2. JUSTIFICATIVA

2.1. A fundamentação da presente contratação e de seus quantitativos, assim como a descrição da solução como um todo, encontram-se pormenorizadas no Formulário - Estudos Preliminares 2643385.

3. ESPECIFICAÇÃO E FORMA DE EXECUÇÃO DO OBJETO

3.1. DESCRIÇÃO DO OBJETO

Grupo	Item	Descrição	Unidade de Fornecimento	Aquisição Inicial	Quantidade a ser Registrada
Único	1	Subscrição de solução de proteção DNS, com garantia técnica de 12 (doze) meses	Subscrições por usuário por 12 (doze) meses	2.000	46.534
	2	Instalação, configuração e transferência de conhecimento relativa ao item 1 desta tabela.	Unidade	1	28

3.1.1. Detalhamento do objeto:

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

3.1.1.2. O objeto é considerado serviço comum pois padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado.

3.1.2. A empresa deverá encaminhar proposta de preços especificando marca e modelo do produto ofertado.

3.1.3. A contratada será responsável pela instalação, integração e funcionamento da solução utilizada na composição de proteção DNS.

3.1.4. Não será aceita a utilização de software livre, software grátis e software de código aberto (open source) na composição da solução de proteção DNS.

3.1.5. A instalação de qualquer componente fornecido do objeto deverá prever a aplicação de todas as correções publicadas e divulgadas pelo fabricante, durante o prazo de garantia.

3.1.6. Para atender aos requisitos solicitados no item 3.1.1 deste Termo de Referência, caso sejam necessários componentes e/ou programas, cujas funcionalidades extrapolem o aqui especificado, estes deverão ser entregues conjuntamente com a solução fornecida, sem requerer licenças externas adicionais e ônus por parte do Contratante.

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

4. PRAZO E LOCAL DE ENTREGA

4.1. As subscrições deverão ser entregues em nome do CONTRATANTE no site do fabricante.

4.1.1. Ao Tribunal Superior Eleitoral fica reservado o direito de recusar de pronto o bem que flagrantemente não esteja em conformidade com a especificação deste Termo de Referência, ressalvado o disposto no item 8.1.3.3 deste Termo.

4.1.2. A Contratada será responsável pela entrega das subscrições no prazo máximo de 20 (vinte) dias corridos contados da notificação do contratante, após o início da vigência do contrato. As subscrições deverão ser entregues em formato digital, por e-mail, ou para download em site do fabricante do produto.

4.1.2.1. A notificação será enviada pela Fiscalização do contrato em até 10 (dez) dias úteis contados do início da vigência do contrato.

4.1.3. Os serviços de instalação, configuração e transferência de conhecimento deverão ser executados de acordo com o cronograma de execução contido no item 7.1 deste Termo de Referência.

4.1.4. Os serviços de instalação, configuração e transferência de conhecimento serão prestados no TSE, localizado no Setor de Administração Federal Sul - SAFS, Quadra 7, Lotes 1 e 2, Brasília – DF, em dias úteis, no horário entre 10h e 18h.

5. GARANTIA TÉCNICA

5.1. A garantia técnica deverá ser prestada durante 12 (doze) meses a partir da entrega das subscrições.

5.2. Os serviços de garantia pertinentes ao Objeto deverão ser realizados por técnicos do fabricante ou por técnicos da Contratada, certificados na solução.

5.3. Deverá ser executado nas modalidades remota e/ou presencial e englobar solução de problemas na ferramenta fornecida. A referida garantia técnica deverá ser prestada no regime 24x7 (vinte e quatro horas por dia, sete dias por semana), durante horário comercial, considerando o fuso horário do contratante.

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

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

5.6. Os prazos referidos nos itens 5.3 e 5.4 são contabilizados de maneira contínua, ou seja, não são interrompidos em função do regime de atendimento 24x7 (vinte quatro horas por dia, sete dias por semana). Uma vez aberto o chamado, deverão ser observados os prazos de atendimento e solução. A critério do contratante, poderá ser solicitado que o atendimento seja interrompido e tenha continuidade no próximo dia útil.

5.7. O tempo máximo para implementação de contorno para problemas é de 6 (seis) horas, contados da abertura do chamado, ultrapassado o prazo limite de 6 (seis) horas, será aplicada penalidade conforme definido no Quadro de Infrações Administrativas.

5.8. O tempo máximo para implementação de solução definitiva para problemas é de 7 (sete) dias, contados da abertura do chamado, ultrapassado o prazo limite de 7 (sete) dias, será aplicada penalidade conforme definido no Quadro de Infrações Administrativas.

5.9. Caso o problema seja bug da ferramenta, deverá ser implementada uma solução de contorno e o prazo para solução definitiva deverá ser acordado com o contratante, não podendo ultrapassar 15 dias.

5.10. 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.

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

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

5.13. As atualizações de software nos componentes e sistemas da solução poderão ser

executadas remotamente, mediante autorização prévia do contratante.

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

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

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

6. FORMAS DE COMUNICAÇÃO E ACOMPANHAMENTO DA EXECUÇÃO DO CONTRATO

6.1. A comunicação entre o TSE e a Contratada durante a execução do contrato, far-se-á, preferencialmente, por meio do preposto designado pela contratada.

6.2. Poderão ser utilizados para a comunicação:

6.2.1. Ofícios;

6.2.2. Mensagens escritas;

6.2.3. Relatórios de Medição e Relatórios em geral;

6.2.4. Termos de Recebimento;

6.2.5. Cartas; e

6.2.6. Demais documentos previstos em contrato ou neste Termo de Referência.

6.3. Sem prejuízo da necessidade de realização de reuniões periódicas, as comunicações devem se dar, preferencialmente, da seguinte maneira:

6.3.1. Questões administrativas durante a execução do contrato, que exijam comunicação formal:

1. Meio de Comunicação: correspondência física ou eletrônica, com aviso e/ou confirmação de recebimento, pessoalmente, por correio, ou por sistema informatizado de correio eletrônico;
2. Periodicidade: eventual ou conforme prazos previstos em contrato ou neste Termo de Referência.

6.3.2. Questões técnicas e/ou administrativas cotidianas, durante a execução do contrato:

1. Meio de Comunicação: correspondência eletrônica, telefone, sistemas ou qualquer outra forma acordada entre as partes, definidas na reunião inaugural;
2. Periodicidade: sempre disponível, em dias úteis, entre 9h e 19h.

6.3.3. Garantia Técnica:

1. Meio de Comunicação: página web, sistema informatizado, correspondência eletrônica, telefone (0800 ou Discagem Local);
2. Periodicidade: tempo integral (24 horas por dia, 7 (sete) dias por semana, 365 dias no ano).

7. CRONOGRAMA DE EXECUÇÃO

7.1. 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	Recebimento de notificação do Contratante para entrega das subscrições	Contratante e Contratada	Recebimento da notificação pela Contratada.
D+5	Reunião de Planejamento	Contratante e Contratada	Ata de reunião assinada.
D+20	Entrega das Subscrições	Contratada	Emissão do Termo de Recebimento Provisório.
D + 60	Concluir instalação, configuração e transferência de conhecimento da solução à equipe Contratante	Contratada	Solução implantada e funcionando plenamente.

7.2. Os prazos de adimplemento dos eventos listados acima, de responsabilidade da contratada, admitem uma única prorrogação, por igual período, em caráter excepcional, sem efeito suspensivo, devendo a solicitação ser encaminhada por escrito, com antecedência mínima de 7 (sete) dias corridos do seu vencimento, anexando-se documento comprobatório do alegado pela contratada, ficando a aceitação da justificativa a critério do TSE e sem prejuízo da aplicação das sanções previstas no instrumento contratual, caso convier, ressalvadas situações de caso fortuito e força maior.

7.3. A Fiscalização Técnica do contrato manifestar-se-á quanto à solicitação no prazo de até 2 (dois) dias úteis. O pedido de prorrogação deverá conter, ao menos:

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

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

8. RECEBIMENTO E PAGAMENTO

8.1. RECEBIMENTO

8.1.1. As subscrições recebidas terão duração de 12 meses e deverão ser entregues em até 20 (vinte) dias corridos contados da notificação para entrega das subscrições.

8.1.2. Em um prazo de até 2 (dois) dias úteis contados do recebimento das subscrições referentes ao item 1, com fundamento no que foi observado ao longo do acompanhamento e da fiscalização técnica do contrato, será emitido o Termo de Recebimento Provisório - TRP por servidor ou comissão previamente designados, quando verificado o cumprimento das exigências previstas na Lista de Verificação correspondente, contida no Anexo I-III deste Termo de Referência.

8.1.3. Após o o recebimento do item 2, o fiscal técnico ou comissão designada terão o prazo de 5 (cinco) dias úteis para emitir o Termo de Recebimento Definitivo - TRD e remeter o processo ao fiscal administrativo. O TRD compreenderá a verificação da conformidade do objeto aos termos contratuais, com fundamento no trabalho feito pelo gestor ou pelo fiscal técnico e na verificação dos outros aspectos do contrato que não a execução do objeto propriamente dito, por meio das análises e conclusões dos quesitos previstos na Lista de Verificação, Anexo I-III deste Termo de Referência.

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

8.1.3.2. Identificada qualquer irregularidade pela fiscalização durante

o recebimento do objeto, a Contratada deverá substituir os bens reprovados e cumprir as obrigações pendentes no prazo de 3 (três) dias úteis, contados da notificação.

8.1.3.3. Decorrido o prazo ou sanada a incorreção apontada pela fiscalização será reiniciado o prazo para emissão do TRD, nos termos do item 8.1.3.

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

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

8.1.3.6. O fiscal técnico ou a comissão designada, no caso de controvérsia sobre a execução do objeto quanto à dimensão, qualidade e/ou quantidade, deverá indicar, no TRD, a parcela incontroversa, a qual deve ser liberada para pagamento, nos termos do art. 143 da Lei nº 14.133/2021, sem prejuízo da aplicação das penalidades previstas no instrumento contratual.

9. PAGAMENTO

9.1. O pagamento será efetuado até o 10º (décimo) dia útil, após o 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. 141 da Lei nº 14.133/21.

9.1.1. O atesto do objeto contratado será feito pelo fiscal administrativo, designado pela autoridade competente, por meio da emissão de Nota Técnica de Atesto (NTA). O fiscal administrativo terá o prazo de 2 (dois) dias úteis para emitir a NTA e remeter o processo à unidade técnica responsável pelo pagamento, a partir do recebimento do documento fiscal, acompanhado do Termo de Recebimento Definitivo - TRD e dos demais documentos exigidos em contrato para liquidação e pagamento da despesa.

9.1.2. Ficará suspenso o prazo para emissão da NTA, pelo período definido pela fiscalização, nos casos em que a Contratada for notificada a apresentar esclarecimentos e documentos. Após o prazo estabelecido, caso a contratada não sane as pendências, a fiscalização administrativa indicará a correspondente ressalva na NTA, e a liquidação poderá seguir com possibilidade de aplicação de glosas/sobrestamentos, até que haja os devidos esclarecimentos/comprovações.

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

9.1.4. O pagamento a ser efetuado em favor da **CONTRATADA** estará sujeito à retenção na fonte de tributos e contribuições sociais de acordo com os normativos legais.

9.1.5. O pagamento das subscrições será feito após emissão do TRD.

9.1.6. O pagamento da instalação, configuração e transferência de conhecimento será feito após emissão do TRD, em parcela única.

10. OBRIGAÇÕES

10.1. OBRIGAÇÕES DA CONTRATADA

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

10.1.2. Responsabilizar-se pelas despesas decorrentes da execução do objeto deste Termo de Referência.

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

10.1.4. Informar, no momento da formalização da contratação, o nome do responsável (preposto), os contatos de telefone, e-mail ou outro meio hábil para comunicação com o TSE, bem como manter os dados atualizados durante toda a execução contratual, conforme Anexo I-IV deste Termo e observado o disposto no Capítulo 6 deste Termo de Referência.

10.1.5. Acatar as recomendações efetuadas pelo fiscal do contrato.

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

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

10.1.8. Comunicar ao TSE, imediatamente, por escrito, 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.

10.1.9. Manter o caráter confidencial dos dados e informações obtidos por qualquer meio ou prestados pelo TSE, 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, observados ainda, no que couber, as diretrizes vigentes adstritas à LGPD (Lei Geral de Proteção de Dados) e a Resolução CD/ANPD nº 2/2022, conforme disposto na Cláusula Dez-DA PROTEÇÃO DE DADOS do instrumento de contrato.

10.1.10. 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 Portal Nacional de Contratações Públicas (PNCP), bem como informar durante toda a vigência qualquer alteração que venha a ocorrer na referida relação.

10.1.11. Manter, durante a execução do contrato, as condições de habilitação exigidas para a contratação.

> **10.1.11.1.** 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.

10.1.12. Responsabilizar-se pelos encargos trabalhistas, previdenciários, fiscais e comerciais resultantes da execução do contrato.

> **10.1.12.1.** A inadimplência da contratada em relação aos encargos suportados não transferirá à Administração a responsabilidade pelo seu pagamento e não poderá onerar o objeto do contrato, nem restringir a regularização e o uso das obras e das edificações, inclusive perante o registro de imóveis.

10.1.13. No caso de fornecimento de bens importados, a contratada deverá apresentar a documentação que comprove a origem dos bens e a quitação dos tributos de importação a eles referentes.

10.1.14. Orientar seus funcionários acerca da necessidade de observar os protocolos sanitários definidos pelo Contratante..

10.1.15. Fornecer máscaras N95 aos seus funcionários, em quantidade suficiente, para ingresso e permanência nas dependências do TSE, quando houver a exigência do uso por parte do Tribunal.

10.1.16. Afastar os funcionários que apresentarem sintomas de doenças infectocontagiosas, sem prejuízo da prestação dos serviços.

10.2. OBRIGAÇÕES DO CONTRATANTE

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

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

10.2.3. Acompanhar, fiscalizar e atestar a execução contratual, bem como indicar as ocorrências verificadas, nos termos de normativo do TSE que disponha sobre os processos de contratação no âmbito do Tribunal.

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

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

10.2.6. Receber a Contratada para reunião inaugural, conforme prazo definido no item 7.1 (Cronograma de Execução).

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

11. DISPOSIÇÕES GERAIS

11.1. PRAZO DE VIGÊNCIA DO CONTRATO

11.1.1. Os contratos decorrentes da ata de registro de preço terão vigência a partir da data de publicação de seu extrato no Portal Nacional de Contratações Públicas (PNCP) e duração de 12 (doze) meses, podendo ser prorrogado conforme Art. 107 da Lei 14.133/2021.

11.1.2. A Ata de Registro de Preços terá vigência a partir da data de publicação de seu extrato no Portal Nacional de Contratações Públicas (PNCP) e duração de 01 (um) ano, podendo ser prorrogada, por igual período, nos termos da Lei.

11.2. CRITÉRIOS DE SUSTENTABILIDADE

11.2.1. Comprovar, como condição para participação na licitação, não possuir inscrição no cadastro de empregadores que tenham submetido trabalhadores a condições análogas à de escravo (Portaria Interministerial MTPS/MM/IRDH nº 4/2016).

11.2.1.1. A comprovação desse critério será efetuada a partir da consulta ao Cadastro acima mencionado, no sítio eletrônico (https://www.gov.br/trabalho-e-emprego/pt-br/assuntos/inspecao-do-trabalho/areas-de-atuacao/cadastro_de_empregadores.pdf), no qual consta lista emitida pelo Ministério do Trabalho e Emprego.

11.2.2. Comprovar, como condição para contratação, não ter sido condenada, a adjudicatária e 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 previsto nos arts. 1º e 170 da Constituição Federal de 1988; no art. 149 do Código Penal; no Decreto nº 5.017/2004 (promulga o Protocolo de Palermo) e nas Convenções nºs 29 e 105 da Organização Internacional do Trabalho.

11.2.2.1. Deverá ser apresentada Certidão Judicial de Distribuição ("nada consta" ou "certidão negativa"), **da esfera criminal, da Justiça Comum (Federal e Estadual)** da adjudicatária e de seus dirigentes.

11.2.3. Comprovar, como condição para participação na licitação, caso a empresa possua 100 (cem) ou mais empregados, atender ao disposto no art. 93 da Lei nº 8.213/91, que determina a obrigatoriedade do preenchimento de 2 a 5% dos seus cargos com beneficiários reabilitados ou com pessoas com deficiência habilitadas, na seguinte proporção:

I - até 200 empregados: 2%;

II - de 201 a 500: 3%;

III - de 501 a 1.000: 4%; e

IV - de 1.001 em diante: 5%.

11.2.3.1. A comprovação será feita mediante declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, nos termos do Inciso IV do Art. 63 da Lei 14.133/2021.

11.2.3.2. Sempre que solicitado pela Administração, a contratada deverá comprovar o cumprimento da reserva de cargos a que se refere o item 11.2.3, com a indicação dos empregados que preencherem as referidas vagas.

11.2.4. Tendo em vista as particularidades técnicas dos serviços a serem contratados, a Contratada, sempre que possível, está desobrigada de apresentar ou comprovar a entrega de serviços de forma impressa. Dessa maneira, sempre que possível, os documentos resultantes da contratação serão apresentados em formato eletrônico.

11.3. SUBCONTRATAÇÃO

11.3.1. É vedado transferir a outrem, no todo ou em parte, o objeto da presente contratação.

ANEXO I-I - ESPECIFICAÇÕES TÉCNICAS

12. ITEM 1 - Subscrição de solução de proteção DNS, com garantia técnica de 12 meses.

12.1. A solução deve implementar a função de DNS Recursivo, ou seja, ser capaz de resolver nomes para IP de forma recursiva utilizando o protocolo DNS sem a necessidade de alterações de código, drivers, pilhas TCP/IP ou substituição do cliente padrão presente nos sistemas operacionais;

12.1.1. A solução fornecida pela CONTRATADA deverá ser baseada em "nuvem", fazendo uso de appliance virtual, a ser executado na infraestrutura do CONTRATANTE, possibilitando a detecção da origem da requisição dos clientes, bem como a realização dos bloqueios localmente;

12.2. Deve possuir licenciamento válido, garantia e suporte técnico do fabricante por 12 (doze) meses;

12.3. A solução deverá ser ofertada em nuvem, todos os componentes necessários para seu funcionamento deverão ser disponibilizados;

12.4. A referida appliance virtual será executado na infraestrutura existente no ambiente do CONTRATANTE;

12.4.1. Caso sejam utilizados appliances, a solução deve ser entregue com appliances virtuais, devidamente licenciados;

12.4.1.1. Os appliances virtuais devem ser compatíveis, no mínimo, com VMware versões 6.5, 6.7 e 7.0;

12.4.1.2. Cada appliance deve ser capaz de tratar, pelo menos, 1.500 consultas de DNS por segundo. Caso o desempenho seja inferior a essa capacidade, deverão ser fornecidos appliances adicionais sem ônus adicional para a CONTRATANTE.

12.4.2. A solução deve implementar mecanismos de alta disponibilidade que não exijam reconfigurações de appliances e agentes e intervenções manuais na solução;

12.4.2.1. A comunicação do agente com a nuvem deve ser autenticada e criptografada.

12.4.2.2. Os serviços em nuvem devem estar localizados em pelo menos 02 (dois) continentes, contendo pelo menos 01 (um) Datacenter no Brasil;

12.4.2.3. Para integração da infraestrutura da CONTRATANTE diretamente com a solução em nuvem, a implantação da solução deve ser através da configuração de DNS Forwarder nos servidores internos de DNS da CONTRATANTE, qualquer que seja o sistema operacional ou solução de servidores de DNS, incluindo servidores Windows, Linux, roteadores, firewalls, switches ou outros equipamentos;

12.4.2.4. Para integração com a infraestrutura da CONTRATANTE utilizando appliances virtuais, a implantação dos appliances deve ser através da configuração via DHCP utilizando o atributo de DNS Server;

12.4.2.5. A solução na nuvem deve operar sem a necessidade de instalação de software ou componentes na infraestrutura interna da CONTRATANTE, exceto: com a instalação de máquinas virtuais na rede da CONTRATANTE (rede corporativa interna ou tenant na nuvem) para receber as requisições DNS e permitir a identificação de cada dispositivo. Neste caso, a CONTRATANTE fornecerá a infraestrutura para operação das máquinas virtuais. Ou com instalação de agentes nos dispositivos (computadores e dispositivos móveis);

12.5. A solução deve permitir identificar em cada requisição de resolução de nomes o IP interno (privado) da estação, servidor e qualquer outro dispositivo conectado a LAN ou WLAN;

12.6. A solução deve permitir visualizar o IP interno (privado) de uma estação mesmo quando esta estação estiver utilizando NAT (Network Address Translation);

12.6.1. É admitido o uso de agente na estação do usuário para esta identificação;

12.7. Se a solução necessitar o uso de agentes, estes devem ser licenciados para todos os usuários da CONTRATANTE;

12.7.1. Os agentes devem ser compatíveis com sistemas operacionais Windows 10 e 11 e superiores e Mac OS X 12 e superiores;

12.8. A solução deve ser capaz de encaminhar resoluções de domínios customizados para servidores internos da CONTRATANTE, incluindo domínios internos e consulta reversa de DNS;

12.9. O fabricante da solução deve possuir centro de inteligência contra ameaças em escala global, com mecanismo dinâmico de reputação de domínios, operando 24x7, todos os dias do ano, conectado a diversas fontes de informações sobre atividades e comportamentos na Internet, incidentes de segurança, capaz de realizar análises de malwares, ransomwares e outros agentes maliciosos com atualizações constantes de proteção;

12.10. A solução deve possuir mecanismos disponíveis que permitam a identificação, além de desabilitar as assinaturas associadas ao falso;

12.11. A solução deve ser efetiva e permanecer ativa em todo momento, independentemente da conectividade do cliente;

12.12. Os dispositivos remotos (fora do ambiente da CONTRATANTE) devem poder utilizar o serviço sem que haja necessidade de conectividade com a rede interna da CONTRATANTE;

12.13. A solução de filtro de DNS deverá funcionar para os dispositivos remotos em qualquer combinação de configuração a seguir: com dispositivos conectados via VPN ou não e operando em split tunneling ou não;

12.14. Deve permitir, no mínimo, duas maneiras de funcionamento:

12.14.1. Por meio de agente instalado no dispositivo;

12.14.2. Configuração de servidor DNS utilizado pelo dispositivo;

12.15. Deve possuir inteligência de ameaças atualizada de forma contínua em escala global (Internet) e customizada, criando um mecanismo dinâmico de reputação além de recursos padronizados de forma estática;

12.16. Dever causar impacto mínimo de performance para o usuário e no endpoint;

12.17. Deve operar nativamente e permitir o uso de uma política geral de segurança na camada DNS;

12.18. Deve integrar de forma simples no sistema de DNS atual do ambiente de produção, especificamente substituindo as referências de servidores recursivos externos em uso;

12.19. Deve permitir proteger todas as plataformas cliente e servidor do ambiente que utilizem comunicação internet através de resolução DNS;

12.20. Deve implementar proteção dos dispositivos em roaming em IPv4 e IPv6, enviando os requests DNS criptografados até a nuvem;

12.20.1. Essa proteção deve permanecer quando o usuário estiver dentro e fora da rede corporativa, sem impacto para as demais políticas de segurança configuradas para o local do usuário;

12.20.2. É admitido o uso de agente instalado nas estações;

12.20.3. Deve utilizar TLS com versões atualizadas para criptografia da comunicação entre agente e nuvem;

12.20.4. Deve detectar quando o usuário está conectado em uma rede confiável via Virtual Appliance e não redirecionar o tráfego;

12.20.5. Deve prover página de onde o administrador possa baixar o perfil de configuração do agente para o ambiente contratado.

12.21. Suportar todos os tipos de dispositivos, estações de trabalho, servidores, dispositivos móveis, sensores e outros dispositivos IoT, appliances e outros, gerenciados e não gerenciados, que se comunicam com a Internet e utilizam o protocolo DNS;

12.22. Deve disponibilizar em uma única console recursos de visibilidade, prevenção e contenção de infecções malware no ambiente local e usuários remotos;

12.23. Deve implementar a prevenção (bloqueio) de malware avançado em diversos vetores de ataque, abrangendo no mínimo e-mail e acesso Web;

12.24. Deve bloquear tráfego de Comando e Controle (C&C, C2, CallBack, PhoneHome) para evitar exfiltração de dados e outros mecanismos de controle remoto implementados por malware e botnets;

12.25. Deve possuir a capacidade de estabelecer reputação, tagging e inteligência de domínios por mecanismos preditivos e dinâmicos, utilização de modelagem estatística, Aprendizado de Máquina (Machine Learning) e aproveitamento automático de utilização de domínios globalmente;

12.26. Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas e domínios por modelos automáticos de co-ocorrência em escala global (concorrência de acessos);

12.27. A solução deve utilizar e correlacionar informações relacionadas aos domínios incluindo, pelo menos, IPs para onde aquele domínio resolve, outros domínios que resolvem para os mesmos IPs, usuários que registraram aquele domínio e outros domínios, Autonomous Systems que detêm os IPs relacionados e histórico de alterações da resolução do domínio;

12.28. A solução deve ser capaz de reconhecer padrões de ataques para proteção contra domínios maliciosos novos ou desconhecidos, classificando de maneira diferenciada domínios recém observados e permitindo bloquear o acesso a eles;

12.29. Deve realizar a detecção e prevenção de DGA's (Domain Generation Algorithm) em tempo real, permitindo a obtenção de inteligência e elementos de correlação com outras infraestruturas globais em uso no contexto observado;

12.30. Deve aplicar controle de acesso a domínios DoH/DoT (DNS sobre HTTPS) aplicando controle ao risco do aumento do uso do DoH e reverter as solicitações DoH para requisições de DNS confiáveis;

12.31. Deve fornecer ferramentas de análise forense de sobre ameaças, como amostras de malware encontradas, grau de risco, co-ocorrências com outros domínios, , para ajudar os analistas a avaliar melhor o escopo, a triagem e a resposta às ameaças;

12.32. Deve prover ferramenta de inteligência de domínios que permita monitorar e identificar domínios semelhantes;

12.33. Deve prover para os domínios investigados as informações de WHOIS, o número do AS, país de criação, score de risco, amostras de malware associadas;

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

12.35. Deve suportar o uso de API programável e documentada para consulta, integração e complemento de inteligência de ameaças com sistemas externos;

12.36. Deve disponibilizar API (Application Programming Interface) de integração com as principais soluções de SOAR (Security Orchestration Automation and Response) de mercado, pela qual seja possível obter reputação de domínio, buscar por detalhes do domínio utilizando expressões regulares para acessar domínios relacionados, histórico de DNS e recorrências (timeline), buscar domínios maliciosos e informações de DNS para um endereço IP (Internet Protocol Address).

12.37. Não deve conflitar com nenhum sistema antivírus local ou posicionado em gateway;

12.38. Quando a consulta de resolução de domínio for para domínios seguros, o serviço deve ser transparente para o usuário final, resolvendo o domínio para a resposta correspondente;

12.39. Proteger contra exfiltração de dados baseado em DNS em todos os tipos de queries de DNS como (A, AAAA, TXT, NS, SOA, CNAME, MX, DNSKEY etc);

12.40. O mecanismo de proteção proativo e automático atuante na monitoração em tempo real da solução durante as pesquisas DNS não pode ser um elemento tipo add-on, ou seja, deve ser uma funcionalidade núcleo da solução, que não dependa de repasse de ações de bloqueio para sistemas externos como firewalls, IPS ou proxy no controle de acesso;

12.41. A solução deve incorporar a capacidade de controle de acesso por categorias implementado em nível DNS mesmo quando não relacionadas à segurança;

12.42. Deve permitir a criação de políticas de segurança com base nos endereços IP

públicos utilizados pelos servidores de DNS locais;

12.43. Deve permitir a definição de listas personalizadas de acesso, para permitir (whitelisting) e para bloqueio (blacklisting), incluindo a capacidade de fazer o upload delas;

12.44. Deve permitir a criação de objetos para identificação de redes internas a partir dos IPs privados;

12.45. Deve permitir a criação de objetos para identificação de redes a partir do IP público;

12.45.1. Deve permitir estabelecer configurações que viabilizem a monitoração, prevenção e controle em redes remotas onde o endereçamento Internet mude em intervalos de tempo (dinâmico);

12.46. Deve permitir a criação de políticas atribuídas a objetos de redes de IPs privados e públicos;

12.47. Deve permitir a criação de múltiplas políticas de segurança com diferentes critérios de seleção com base no IP interno, IP público, usuário, grupo de usuário, estação de trabalho, segmento de rede;

12.48. As políticas de segurança devem fornecer, pelo menos, as seguintes funcionalidades:

12.48.1. Opção de bloqueio de domínios relacionados com artefatos maliciosos e domínios comprometidos, independente da aplicação, protocolo ou porta utilizada pela aplicação;

12.48.2. Opção de bloqueio de domínios de serviços de DDNS (Dynamic DNS);

12.48.3. Opção de bloqueio de domínios recentemente ativados;

12.48.4. Opção de bloqueio de domínios potencialmente nocivos que apresentam comportamento suspeito e possam estar relacionados a ameaças;

12.48.5. Opção de bloqueio de domínios utilizados para túneis sobre o protocolo DNS (DNS Tunneling VPN);

12.48.6. Opção de bloqueio de domínios relacionados a botnets e redes de Comando e Controle (C2), independente da aplicação, protocolo ou porta da aplicação;

12.48.7. Opção de bloqueio de domínios relacionados com phishing ou fraudes para obter dados pessoais ou financeiros;

12.48.8. Opção de bloqueio de domínios com base na classificação da categoria do domínio;

12.48.8.1. Deve suportar, no mínimo, as seguintes categorias: *Command & Control callbacks, Malware, Phishing, Cryptomining, Pornography, Gambling, Illegal Activities, Terrorism, Proxy/Anonymizer, Personal VPN* ou equivalentes.

12.48.9. Opção de bloqueio de domínios utilizados para mineração de criptomoedas;

12.48.10. Opção de bloqueio de aplicativos incluindo, pelo menos, os aplicativos Anonymizers, Amazon Drive, Dropbox, Box, Google Drive, Mega, Microsoft OneDrive, BitTorrent, Amazon Video, Google Play Movies, Google Play Music, HBO Now, Netflix, Spotify, YouTube e Twitch;

12.48.11. Opção de permissão de aplicativos que foram bloqueados por determinadas categorias, incluindo, pelo menos, os aplicativos listados no item anterior;

12.48.12. Permitir a criação de listas brancas (whitelist) e listas negras (blacklist) globais de domínios, ou seja, aplicada a todas as políticas, e específicos por política de segurança;

12.48.13. Permitir que políticas de segurança funcionem em modo restrito permitindo somente acessos a domínios de uma lista branca;

12.49. As alterações de configuração das políticas de segurança devem ser efetivadas imediatamente, sem necessidade de atualização de bases ou assinaturas nos appliances e agentes;

12.50. O bloqueio aos domínios maliciosos deve ser implementado através da resposta da consulta DNS para um IP seguro;

12.51. A solução deve permitir o controle de acesso baseado em políticas que incorporem identidades como elementos de decisão de contexto de acesso, incluindo os decorrentes de

capacidade de integração com Microsoft Active Directory como:

12.51.1. Usuários;

12.51.2. Grupos;

12.51.3. Sistemas/endpoints;

12.51.4. Redes, IP's, CIDR;

12.52. A solução não deve depender de listas locais, feeds, antivírus ou proxies para:

12.52.1. Manutenção e automação do conteúdo das categorias de segurança padrão;

12.52.2. Prover visibilidade e detecção de condições de "Fast Fluxing" (redes utilizadas por várias botnets para esconder os domínios utilizados para baixar malware ou hospedar sites web com phishing) de infraestruturas e domínios suspeitos, maliciosos e dinâmicos;

12.52.3. Prover visibilidade e prevenção de exposição contra ataques incorporando "Domain-Shadowing" (processo de criação de subdomínios por proprietários de domínio usando credenciais) e cadeias de acesso aos portais de distribuição de malware e ataques;

12.53. A solução deve ser acessível para usuários localizados na rede local da CONTRATANTE e remotamente, de qualquer local conectado à Internet, sendo admitida a instalação de agentes nas estações de trabalho remotas;

12.53.1. Não serão aceitas soluções que, para atender usuários remotos, exijam que os appliances localizados na CONTRATANTE sejam disponibilizados para acesso direto via Internet;

12.53.2. Deve ser fornecida, sem ônus adicional para a CONTRATANTE, toda a infraestrutura incluindo hardware, software, licenças e assinaturas e demais componentes em alta disponibilidade necessários para o uso da solução por usuários remotos;

12.53.3. A comunicação do agente com a nuvem deve ser autenticada e criptografada;

12.54. A utilização da solução por usuários localizados na rede LAN ou WLAN não deve exigir a instalação de agentes;

12.55. Deve ser licenciado para todos os usuários corporativos, independentemente do local de trabalho;

12.56. Deve permitir a personalização de múltiplas páginas de bloqueio de acesso e uso em distintas políticas de forma simultânea;

12.57. Caso o usuário esteja utilizando um navegador web através de HTTP e HTTPS, a solução deve exibir uma página indicado o motivo do bloqueio:

12.57.1. Deve permitir a definição de um texto que deve ser apresentado na página de bloqueio;

12.57.2. Permitir a criação de páginas personalizadas diferenciadas por tipo de bloqueio, incluindo bloqueios por categoria, lista negra, phishing e política de segurança;

12.57.3. Permitir a configuração de uma URL para redirecionamento do usuário;

12.57.4. Permitir a configuração de um formulário para contato com o administrador;

12.57.5. Para acesso utilizando HTTPS, a solução deve disponibilizar o certificado utilizado para criptografia da sessão ou permitir a importação de um certificado e a chave privada correspondente;

12.58. Todas as configurações do serviço devem ser realizadas através de ferramenta gráfica a partir de um portal com acesso via web utilizando protocolo seguro (HTTPS);

12.59. Permitir o acesso simultâneo de múltiplos administradores.

12.60. Permitir a criação de administradores com perfis de acesso total, somente leitura e somente geração de relatórios.

12.61. Deve permitir que condições de bloqueio sejam tratadas de forma diferente, incluindo recursos de by-pass configurável por usuários e códigos com tempos de duração preestabelecidos para contextos específicos de acesso e categorias;

12.62. Deve permitir integração para SSO (Single Sign-On) através do padrão aberto SAML (Security Assertion Markup Language) para autenticação com provedores SAML. A solução deverá suportar a integração com o Cisco DUO, atualmente em uso no ambiente do

CONTRATANTE:

12.63. Não deve conflitar com nenhum sistema sandbox posicionado como endpoint em segmentos de rede ou plataforma gateway;

12.64. Não deve precisar de um mecanismo de firewall para bloqueio de exposição a ameaças em tempo real;

12.65. Não deve precisar de integração com proxy para bloqueio de ameaças em tempo real;

12.66. Não deve ser uma solução para configuração, manutenção, implementação e serviço de DNS autoritativo;

12.67. Não deve ser uma solução para substituição de infraestrutura de DNS interno, serviço DHCP ou firewall;

12.68. Deve nativamente permitir estabelecer detecção, reputação e inteligência de infraestruturas pela monitoração automática de endereçamento IP e suas respectivas ASN incluindo atribuição DNS e correlação WHOIS automática;

12.69. Deve nativamente e automaticamente permitir a monitoração através de uma modelagem contínua que quantifica, estabelece ranking e identifica padrões de utilização de infraestruturas, estabelecendo critérios de detecção e correlação com campanhas e mecanismos direcionados de ataques;

12.70. A solução deve possuir um mecanismo automático de roteamento por Anycast em escala global;

12.71. A solução deve permitir páginas de bloqueio customizáveis, configuração de Bypass ou Sinkhole;

12.72. Deve permitir um mecanismo de busca de inteligência para domínios, IP's, HASH, incluindo a automação destas por uso de API's;

12.73. A solução deverá ser capaz de enviar logs das requisições e dos bloqueios realizados para soluções de SIEM. Suportar, no mínimo, QRadar, Splunk, Microsoft Sentinel e Logrhythm;

12.74. Deve permitir proteger sistemas tento na rede local da CONTRATA quanto em equipamentos em utilização externa, como usuários de Teletrabalho, por exemplo;

12.75. Deve ser capaz de alimentar inteligência de ameaças a plataformas SIEM (Security Information and Event Management);

12.76. Deve ser capaz de monitorar a atividade de rede em tempo real;

12.77. Deve ser capaz de monitorar a utilização de serviços em nuvem (Cloud Services) para identificar riscos e desenvolver atividades de conformidade de forma automática;

12.78. Deve permitir a identificação de ataques direcionados;

12.79. Deve permitir a comparação do tráfego DNS local e utilização de um domínio contra os padrões globais de tráfego;

12.80. Deve permitir a visualização de informações além de endereços IP ou DNS, como o relacionamento inteiro com a ASN (Autonomous System Number);

12.81. Deve permitir exportar logs DNS para um repositório terceiro para análise posterior;

12.82. Deve permitir, nativamente, o uso de inteligência gerada por tecnologia de virtualização de artefatos, sejam suspeitos ou maliciosos, incorporando-o diretamente no processo de defesa proativa em nível DNS de forma automática;

12.83. Permitir a criação de usuários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;

12.83.1. Permitir a criação de códigos temporários com autorização de transpor o bloqueio por categoria de conteúdo e lista de domínios, sem a necessidade de reconfigurar os servidores DNS destes usuários;

12.84. Deve permitir o uso de uma API programável e documentada para:

12.84.1. Automação de envios, pesquisas (query) em históricos e processo de análise;

12.84.2. Automação na utilização de inteligência de ameaças para segurança de DNS, incluindo domínios, IP, URL e hashes de arquivos;

12.85. Deve permitir consolidar, em uma única interface e de forma automática, a correlação de reputação de inteligência DNS de forma individualizada por domínios em escala global com resultados de análise dinâmica e estática de artefatos e indicadores comportamentais para ameaças malware (incluindo Advanced Persistent Threats) em escala global;

12.86. Possuir relatório de informações gerais contendo, pelo menos, as seguintes informações:

12.86.1. Gráfico com total de requisições de resolução de domínios realizadas ao longo do tempo;

12.86.2. Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, categoria e listas ao longo do tempo;

12.86.3. Gráfico com total de requisições de resolução de domínios que foram bloqueadas por critérios de segurança, incluindo malwares, phishings, botnets e outros ao longo do tempo;

12.86.4. Listagem dos, pelo menos, 10 destinos mais solicitados que foram bloqueados e suas quantidades de resoluções;

12.86.5. Listagem dos clientes com mais solicitações e suas quantidades de resoluções;

12.86.6. Listagem dos motivos de bloqueio, com as suas quantidades;

12.86.7. Permitir escolher os períodos destes dados considerando, pelo menos, as janelas de tempo das últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.87. Possuir relatório gráfico com o total de requisições de resolução de domínios ao longo de um período;

12.87.1. Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.87.2. Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;

12.88. Possuir relatório com sumário das requisições informando os bloqueios por critérios de segurança, categorias, listas de bloqueio e as resoluções que foram permitidas normalmente;

12.89. Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;

12.90. Possuir relatório gráfico do volume de requisições de resolução de domínios informando os bloqueios por critérios de segurança, categorias e listas de bloqueio;

12.90.1. Permitir a filtragem por cliente que solicitou a resolução;

12.91. Possuir relatório com listagem dos domínios resolvidos, informando a data e hora da requisição, o cliente, o destino, o IP privado, IP público, tipo de requisição DNS e a resposta;

12.91.1. Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.91.2. Permitir a filtragem por cliente, incluindo segmentos de rede, IPs públicos, agentes e outros, que solicitou a resolução;

12.91.3. Permitir a filtragem por categoria do domínio;

12.91.4. Permitir a filtragem por critério de segurança;

12.91.5. Permitir a filtragem por respostas bloqueadas e permitidas;

12.91.6. Permitir o download do resultado em formato CSV;

12.92. Possuir relatório com listagem dos domínios mais solicitados, apresentando a classificação da categoria do domínio e o volume de requisições;

12.92.1. Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.92.2. Permitir a filtragem por cliente que solicitou a resolução;

12.92.3. Permitir a filtragem por categoria do domínio;

12.92.4. Permitir a busca e filtragem por IP;

12.92.5. Permitir a filtragem por critérios de ameaça e risco dos domínios;

12.93. Possuir relatório com listagem de categorias de domínios mais solicitados, apresentando o volume de requisições;

12.93.1. Permitir filtros para, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.93.2. Permitir a filtragem por cliente que solicitou a resolução;

12.93.3. Permitir a filtragem para resoluções bloqueadas e permitidas;

12.94. Possuir relatório com listagem de origens, incluindo segmentos de rede, IPs públicos, agentes e outros, por quantidade de solicitações, apresentando o volume de requisições

12.94.1. Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.94.2. Permitir a filtragem por cliente que solicitou a resolução;

12.94.3. Permitir a filtragem por categoria do domínio;

12.94.4. Permitir a filtragem por critérios de ameaça e risco dos domínios;

12.95. Possuir relatório por cliente apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas, listagem dos domínios mais acessados, das categorias de riscos e ameaças e das últimas resoluções de nomes realizadas;

12.95.1. Deve exibir o IP público utilizado para resolução;

12.95.2. Deve exibir o IP privado do cliente;

12.95.3. Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.96. Possuir relatório por domínio apresentando gráfico da quantidade de solicitações ao longo do tempo com resoluções bloqueadas e permitidas e comparação com o volume de resoluções feitas por outros usuários do serviço no contexto global para aquele domínio, listagem dos clientes que mais solicitaram resolução, das últimas resoluções de nomes realizadas;

12.96.1. Deve exibir o IP público utilizado para resolução;

12.96.2. Deve exibir o IP privado do cliente;

12.96.3. Permitir filtros de, pelo menos, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.97. Possuir relatório de domínios agrupados por serviços online disponíveis na Internet incluindo, por exemplo, porém, não se limitando a, Office 365, Dropbox, Salesforce, LinkedIn, Google Docs, Reddit, Facebook, Gmail e outros;

12.97.1. Deve informar a classificação do serviço;

12.97.2. Deve informar o volume de solicitações de resoluções realizadas e a quantidade bloqueada;

12.97.3. Deve informar o volume de clientes que fizeram requisições;

12.97.4. Deve informar a data da primeira requisição e a última data;

12.97.5. Permitir filtros de, pelo menos, o dia atual, as últimas 24 horas, o dia anterior, os últimos 7 dias e os últimos 30 dias;

12.97.6. Permitir a filtragem por cliente que solicitou a resolução;

12.97.7. Permitir a filtragem por categoria do domínio;

12.97.8. Permitir a busca por um serviço;

12.98. Possuir relatório de aplicações online identificadas informando o nome da aplicação, o fornecedor da aplicação, a categoria da aplicação e as quantidades de aplicações da mesma categoria;

12.99. Possuir ferramenta de extração de relatórios permitindo busca a partir de:

12.99.1. Tipo de resposta: permitida, bloqueada, lista de bloqueio ou de permissão;

12.99.2. Tipo do cliente: estação de trabalho, usuário, agente, dispositivos de rede, rede ou local;

12.99.3. Categoria da ameaça;

12.99.4. Categoria do domínio;

12.99.5. Permitir a exclusão de domínios que resolvem para CDNs;

12.100. Deve armazenar todos os registros de acesso por pelo menos 30 dias e permitir seu download em formato CSV;

12.101. Deve permitir o agendamento para geração e envio automático de relatórios de, pelo menos, os seguintes tipos:

12.101.1. Listagem das resoluções realizadas, permitindo a filtragem por cliente, domínio, IP de cliente, permissão ou bloqueio, categoria do domínio e risco e ameaça do domínio;

12.101.2. Listagem de eventos de segurança incluindo malware, botnet e outras ameaças e riscos, permitindo a filtragem por cliente, domínio, IP de cliente e risco e ameaça do domínio;

12.101.3. Listagem dos serviços agrupados por domínio, permitindo a filtragem pelo serviço, cliente e a categoria;

12.101.4. Listagem do volume de requisições, indicando permissão ou bloqueio, permitindo filtragem por cliente;

12.101.5. Gráfico do volume total, permitindo filtragem por cliente;

12.101.6. Listagem dos domínios mais resolvidos, permitindo filtragem por cliente, permissão ou bloqueio, domínio, categoria e riscos e ameaça do domínio;

12.101.7. Listagem das categorias mais resolvidas, permitindo filtragem por cliente, permissão ou bloqueio;

12.101.8. Listagem dos clientes que mais fazem requisições de resolução, permitindo filtragem por cliente, categoria e riscos e ameaça do domínio;

12.101.9. Relatório executivo gráfico com o resumo das ameaças bloqueadas, eventos de segurança mais recorrentes e serviços mais acessados;

12.102. Entende-se por cliente qualquer origem da requisição de resolução de nomes, podendo ser um usuário, estação de trabalho, agente, IP público, rede com IP privado ou local, conforme configurações das funcionalidades de segurança;

12.103. O serviço de filtro de DNS deve contemplar todas as funcionalidades, licenças, programas e produtos para atendimento dos requisitos deste edital;

12.104. Esse serviço deve incluir credenciais para o website do Fabricante, onde deverão ser disponibilizadas as últimas versões do(s) programa(s), suas atualizações e correções, e acesso integral às documentações e especificações;

12.105. A CONTRATADA fornecerá ao CONTRATANTE, durante a validade do contrato, acesso às novas versões da solução, correções emergenciais e pacotes de correções de software, sem ônus adicional além dos já previstos em contrato;

12.106. A CONTRATADA deverá prover acesso à CONTRATANTE ao acervo de documentações, especificações e base de conhecimento no site do fabricante da solução.

12.107. O serviço de suporte técnico deverá contemplar toda a solução, incluindo programas ou produtos fornecidos para atendimento dos requisitos do edital;

12.108. Consiste na prestação de serviço de suporte técnico especializado para auxílio no uso da solução, resolução de problemas de mau funcionamento e ajustes de configuração em qualquer funcionalidade da solução;

12.109. O serviço de suporte técnico remoto deve estar disponível de forma ininterrupta, podendo ser acionado 24x7 (vinte quatro horas por dia – durante os sete dias da semana, incluindo feriados);

12.110. A CONTRATADA deverá prover um mecanismo de abertura de chamado através de sistema em site on-line, via web e por telefone no Brasil. Para acesso a este site, serão fornecidas ao CONTRATANTE todas as informações necessárias para ingresso no sistema, inclusive senhas de uso exclusivo.

13. **ITEM 2 -** Serviço de instalação, configuração e transferência de conhecimento.

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

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

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

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

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

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

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

13.8. A instalação será considerada concluída com sucesso após o serviço estar funcionando sem defeitos e com uma política básica e universal com pelo menos as seguintes funcionalidades:

13.8.1. Deve implementar a prevenção (bloqueio) de malware avançado em diversos vetores de ataque, abrangendo no mínimo e-mail e acesso Web;

13.8.2. Deve bloquear tráfego de Comando e Controle (C&C, C2, CallBack, PhoneHome) para evitar exfiltração de dados e outros mecanismos de controle remoto implementados por malware e botnets;

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

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

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

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

13.13. A transferência de conhecimento deverá ser realizada para, no mínimo, 5 (cinco) pessoas que sejam servidores do Contratante;

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

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

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

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

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

13.16. Concluir instalação, configuração e transferência de conhecimento da solução no prazo de 60 (sessenta) dias corridos, contados do recebimento da notificação do Contratante para entrega das subscrições.

13.17. Caso seja de comum acordo entre o Contratante e a CONTRATADA, as atividades remotas relacionadas no item 13 e subitens poderão ser realizadas presencialmente.

ANEXO I-II - MODELO DE PROPOSTA

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

Grupo	Item	Descrição	Unidade de Fornecimento	Quantidade	Valor unitário para 12 meses (R$)	Valor total (R$)
Único	1	Subscrição de solução de proteção DNS, com instalação, transferência de conhecimento e garantia técnica de 12 meses.	Subscrições por usuário	46.534		
	2	Instalação, configuração e transferência de conhecimento relativa ao item 1 desta tabela.	Unidade	28		
	Valor Total do Grupo (R$):					

Declarações:
i) Esta empresa declara que tem pleno conhecimento das condições necessárias para a execução do objeto.
ii) Esta empresa declara que nos preços propostos acima estão incluídas todas as despesas, frete, tributos e demais encargos de qualquer natureza incidentes sobre o objeto da contratação.
iii) Esta empresa declara estar ciente de que a apresentação da presente proposta implica na plena aceitação das condições estabelecidas no Edital e seus Anexos.
iv) Esta empresa declara estar ciente da necessidade de apresentação dos documentos de habilitação exigidos, bem como dos critérios de sustentabilidades a serem comprovados **e dos demais documentos previstos no Edital e seus Anexos.**

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

Observações para o Preenchimento da Proposta pelas Empresas:
1) A tabela da proposta deverá ser ajustada, preenchendo-se as linhas e colunas, com o detalhamento do objeto a ser fornecido, observadas as especificações contidas no Termo de Referência.

ANEXO I-III - LISTA DE VERIFICAÇÃO

TERMO DE RECEBIMENTO PROVISÓRIO

Processo SEI Relacionado:
Contratada:
CNPJ nº:
Contrato TSE nº:
Objeto: Subscrição para solução de proteção DNS para 12 (doze) meses.
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

TERMO DE RECEBIMENTO PROVISÓRIO			
1	A contratada apresentou comprovação de licenciamento em nome do TSE?		
2	A entrega deu-se em conformidade com o prazo contratual?		

RELATÓRIO DE OCORRÊNCIAS

RECEBIMENTO PROVISÓRIO DO OBJETO	
Diante da entrega dos serviços pela CONTRATADA e observada a posterior avaliação detalhada dos aspectos quantitativos e qualitativos a ser efetuada durante o Recebimento Definitivo, essa fiscalização decide por:	
	R E C E B E R 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 (se for o caso):** **Contratada:** **CNPJ nº:** **Contrato/Nota de Empenho:** **Objeto:** **Prazo de Entrega:**
Fiscalização: Memorando nº (SEI nº) **Fiscal Técnico Titular:** **Fiscal Técnico Substituto:**

ITEM	CRITÉRIO DE CONFERÊNCIA	SIM	NÃO	N.A.
1	**ASPECTOS DA AQUISIÇÃO:**			
1.1	O número de licenças fornecido corresponde ao contratado?			
1.2	Os itens de software fornecidos correspondem ao especificado no Termo de Referência?			
1.3	Os prazos de garantia e suporte correspondem ao definido no contrato?			
1.4	A instalação dos softwares deu-se conforme especificado no Termo de Referência?			
	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 Termo de Referência e do instrumento contratual, quanto aos aspectos quantitativos, qualitativos e de obrigações contratuais, a fiscalização decide, ressalvadas eventuais observações contidas no Relatório de Ocorrências, 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 representada pelo seu **Cargo do Representante**, Senhor(a) **Nome do Representante** portador(a) da Carteira de Identidade nº **Identidade do Representante**, CPF nº **CPF do Representante**, em atenção ao art. 44 da IN MPDG nº 5/2017, DESIGNA, o(a) Senhor(a) **Nome do Colaborador**, portador(a) da Carteira de Identidade nº **Identidade do Colaborado**, CPF nº **CPF do Colaborador**, para atuar como preposto no âmbito do **Contrato TSE nº xx/xxxx**.

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

a)	Ser acessível ao Contratante, por intermédio do email e dos números de telefone fixo e celular informados neste formulário.
b)	Acatar as recomendações efetuadas pelo fiscal do contrato.
c)	Participar da reunião inaugural a ser agendada com a fiscalização do contrato.
d)	Comparecer, sempre que solicitado pelo fiscal do contrato, no prazo máximo de 24 (vinte e quatro) horas, para exame e esclarecimentos de quaisquer ocorrências, salvo em situações emergenciais de pronto atendimento.
e)	Agilizar os contatos com os representantes da administração durante a execução do contrato.
f)	Desenvolver outras atividades de responsabilidade da Contratada, principalmente quanto ao controle de informações relativas ao seu contrato e apresentação de documentos quando solicitado.

3. A comunicação entre o preposto e o Tribunal Superior Eleitoral será efetuada por meio dos telefones fixo **(DDD) 00000-0000** e celular **(DDD) 00000-0000** ou do e-mail **email@email.com.br**.
4. A **Nome da Empresa** compromete-se a manter atualizados, durante toda fase de execução da contratação, os contatos de telefone e e-mail para comunicação com o Tribunal Superior Eleitoral.

ANEXO I-V - TERMO DE CONFIDENCIALIDADE

MODELO TERMO DE CONFIDENCIALIDADE

TERMO DE CONFIDENCIALIDADE, VINCULADO AO CONTRATO TSE Nº _____/_____, QUE ENTRE SI CELEBRAM O TRIBUNAL SUPERIOR ELEITORAL E A EMPRESA _____.

O **CONTRATANTE**, **TRIBUNAL SUPERIOR ELEITORAL**, sediado no Setor de Administração Federal Sul - SAFS, Quadra 7, Lotes 1 e 2, Brasília/DF, CNPJ nº 00.509.018/0001-13, representado pelo (a) _____, Senhor(a) _____, portador(a) da Carteira de Identidade nº _____, CPF nº _____ e, de outro lado, a empresa **CONTRATADA**, _____, inscrita no CNPJ/MF sob o número _____, sediada em _____, neste ato, representada por _____, portador(a) da Carteira de Identidade nº _____, CPF nº _____, têm justo e acordado celebrar o presente **TERMO DE CONFIDENCIALIDADE, VINCULADO AO CONTRATO TSE Nº _____/_____,** por meio do qual a **CONTRATADA** compromete-se a observar as

disposições das cláusulas seguintes:

CLÁUSULA PRIMEIRA

DO OBJETO

O presente Termo de Confidencialidade tem por objeto a necessária e adequada proteção às informações confidencias a que a contratada tiver acesso na execução das atividades do Contrato nº _____/202__ contempladas especificamente no respectivo contrato.

Subcláusula primeira – A **CONTRATADA** reconhece que, em razão da prestação de serviços ao TSE, tem acesso às informações pertencentes ao TSE, descritas na Cláusula Segunda, que devem ser tratadas como controladas.

CLÁUSULA SEGUNDA

DAS INFORMAÇÕES CONFIDENCIAIS

As informações controladas abrangem toda informação, por qualquer modo apresentada ou observada, 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, pen drives, 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, entre outras a que, diretamente ou através de seus empregados, prepostos ou prestadores de serviço, venha à **CONTRATADA** ter acesso durante ou em razão da execução do contrato celebrado, incluindo-se, ainda, o presente Termo de Confidencialidade.

Subcláusula primeira – Subcláusula primeira – Em caso de dúvida acerca da natureza confidencial de determinada informação, a **CONTRATADA** deverá entrar em contato com TSE e aguardar o retorno, mantendo sigilo quanto à informação até manifestação expressa do TSE sobre a confidencialidade e permissão de acesso. Em hipótese alguma, a ausência de manifestação expressa do TSE poderá ser interpretada como liberação de qualquer dos compromissos ora assumidos.

CLÁUSULA TERCEIRA

DAS OBRIGAÇÕES

A **CONTRATADA** compromete-se a não utilizar, bem como a não permitir que seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos utilizem, de forma diversa da prevista no contrato de prestação de serviços ao TSE, as informações controladas reveladas.

Subcláusula primeira – A **CONTRATADA** deverá cuidar para 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 controladas reveladas.

Subcláusula segunda – A **CONTRATADA** deverá possuir ou firmar acordos por escrito com seus diretores, consultores, prestadores de serviços, empregados e/ou prepostos cujos termos sejam suficientes a garantir o cumprimento de todas as disposições do presente Termo de Confidencialidade.

Subcláusula terceira – A **CONTRATADA** obriga-se a informar imediatamente ao TSE qualquer violação das regras de sigilo estabelecidas neste Termo de Confidencialidade que tenha tomado conhecimento ou ocorrido por sua ação ou omissão, independentemente da existência de dolo.

CLÁUSULA QUARTA

DO DESCUMPRIMENTO

A quebra do sigilo das informações controladas reveladas, devidamente comprovada, sem autorização expressa do TSE, sujeitará a **CONTRATADA**, por ação ou omissão, ao pagamento de multa de acordo com os percentuais descritos a seguir, observada a natureza e gravidade da violação que deu causa

à aplicação da multa, bem como as responsabilidades administrativa, civil e penal respectivas, as quais serão apuradas em regular processo judicial ou administrativo, possibilitando inclusive a rescisão do Contrato nº _____/202__, firmado entre o TSE e a **CONTRATADA** sem qualquer ônus para o TSE.

- 0,5% a 1% sobre o valor do contrato - para situações de baixa criticidade;

- 2,5% a 5% sobre o valor do contrato - para situações de criticidade média;

- 8% a 10% sobre o valor do contrato - para situações de criticidade alta.

CLÁUSULA QUINTA
DO RETORNO DAS INFORMAÇÕES

A **CONTRATADA** devolverá imediatamente ao TSE, ao término do Contrato, todo e qualquer material de propriedade deste, inclusive registro de documentos de qualquer natureza que tenham sido criados, usados ou mantidos sob seu controle ou posse, bem como de seus empregados, prepostos ou prestadores de serviço, assumindo o compromisso de não utilizar qualquer informação considerada confidencial, conforme este Termo de Confidencialidade, a que teve acesso em decorrência do vínculo contratual com o TSE.

CLÁUSULA SEXTA
DA VIGÊNCIA

O presente termo, de natureza irrevogável e irretratável, terá vigência a partir de sua assinatura, permanecendo em vigor até ____ (meses/anos) após o término do contrato, mantendo-se, da mesma forma, a obrigação de confidencialidade após o encerramento da vigência do contrato, bem como no caso de rescisão contratual.

CLÁUSULA SÉTIMA
DAS DISPOSIÇÕES FINAIS

Os casos omissos neste Termo de Confidencialidade, assim como as dúvidas surgidas em decorrência da sua execução, serão resolvidos pelo TSE.

Por estar de acordo, a **CONTRATADA**, por meio de seu representante, firma o presente Termo de Confidencialidade, assinando-o eletronicamente.

ADAÍRES AGUIAR LIMA
SECRETÁRIA DE ADMINISTRAÇÃO

Documento assinado eletronicamente em **06/09/2024, às 11:17**, horário oficial de Brasília, conforme art. 1º, §2º, III, b, da Lei 11.419/2006.

Tribunal Superior Eleitoral

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=3004049&crc=90329115, informando, caso não preenchido, o código verificador **3004049** e o código CRC **90329115**.
