TRIBUNAL REGIONAL ELEITORAL DO PIAUI

Termo de Referência Nº 113

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

(Processo Administrativo n° 0004596-73.2023.6.18.8000)

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. **CONDIÇÕES GERAIS DA CONTRATAÇÃO**

    1. Aquisição de sistema de filtragem e otimização de conteúdo web via provimento de funcionalidades de "Secure Web Gateway" (SWG), incluindo instalação, configuração, testes operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, bem como os serviços de migração, treinamento, garantia, consultoria e suporte técnico, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	MÉTRICA OU UNIDADE DE MEDIDA	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
1	Solução de Secure Web Gateway	Licença por usuários	1.500	R$ 745,467	R$ 1.118.201,23
2	Suporte	Mensal	36	R$ 3658,306	R$ 131.699,04
3	Treinamento	Turma	1	R$ 42.166,66	R$ 42.166,66

2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

3. O bem objeto desta contratação é caracterizado como comum, uma vez que é possível especificar e medir seu desempenho e qualidade utilizando parâmetros usuais de mercado.

4. O prazo de vigência da contratação é de 03 (três) anos, prorrogável para até 10 (dez) anos, na forma dos artigos 106 e 107 da Lei n° 14.133, de 2021.

    1. O fornecimento do bem é enquadrado como continuado tendo em vista que o s serviços de garantia e suporte técnicos da solução se estende por mais de um ano, pois são necessários para a estabilidade, economia de custos, previsibilidade orçamentária, redução de sobrecarga administrativa, conformidade regulatória e garantia de atualizações consistentes, sendo a vigência plurianual mais vantajosa considerando os Estudos Técnicos Preliminares 5 (0001812006).

5. O Contrato oferece maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2. A solução de TIC consiste no fornecimento, instalação e configuração de sistema de filtragem e otimização de conteúdo web via provimento de funcionalidades de "Secure Web Gateway" (SWG), incluindo testes operacionais, operação assistida e demais componentes necessários ao seu perfeito funcionamento, com licença de uso para 1.500 usuários, bem como os serviços de migração, treinamento, garantia, consultoria e suporte técnico pelo período de 36 (trinta e seis) meses, visando a mitigação do risco de ataques cibernéticos e bloqueio de acesso dos usuários da rede interna deste Tribunal Regional Eleitoral do Piauí a sites e aplicativos maliciosos.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

1. A presente contratação é medida crucial para fortalecer a segurança cibernética e proteger informações confidenciais e ativos de rede deste Tribunal Regional Eleitoral do Piauí. Justifica-se pela crescente e constante sofisticação das ameaças cibernéticas que visam atacar órgãos governamentais, tornando imperativo implementar mecanismo robusto de filtragem de tráfego web.

2. Uma solução de Secure Web Gateway proporciona uma defesa proativa ao bloquear o acesso a sites maliciosos, controlar o tráfego da web, aplicar políticas de uso aceitável e garantir conformidade com regulamentações de segurança e privacidade de dados. Além disso, é capaz de oferecer visibilidade em tempo real das atividades online, permitindo respostas ágeis a incidentes de segurança. Dessa forma, a aquisição de um SWG reforça a postura de segurança cibernética, protege informações sensíveis e assegura a continuidade de operações críticas e o bom desempenho das atividades no âmbito desta Justiça Especializada, elevando a confiabilidade, integridade e a disponibilidade dos serviços oferecidos ao público interno e à sociedade, segundo as melhores práticas do mercado de segurança da informação.

3. O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme

Portaria Presidencial Nº 1.024/TRE/PRESI/DG/ASSDG, de 18 de Novembro de 2022, puiblicado no DOU nº 223, de 28/11/2022, p. 145-147 (1719728).

4. O objeto da contratação também está alinhado com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2021-2026 do Tribunal Regional Eleitoral do Piauí, conforme demonstrado abaixo:

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	**Objetivos Estratégicos**
OE1	Aumentar a Satisfação dos Usuários dos Serviços de TI
OE2	Promover a Transformação Digital
OE5	Aperfeiçoar a Governança e a Gestão de TI
OE7	Aprimorar a Segurança da Informação e Proteção de Dados

4. REQUISITOS DA CONTRATAÇÃO

1. Requisitos de Negócio:

1. A presente contratação orienta-se pelos seguintes requisitos de negócio:
    1. Filtragem de URLs e de reputação "online" do conteúdo "web":
        1. Categorização de "web sites" conhecidos em grupos permitindo o bloqueio.
        2. Obtenção de relatórios de uso com maior grau de detalhe e de especificidade da demanda.
    2. Filtragem de "malwares":
        1. Proteção contra softwares potencialmente maliciosos ("malwares").
        2. Proteção contra softwares não autorizados.
    3. Controles ao nível das aplicações "web":
        1. Gerenciamento de aplicações baseadas na Internet (mensageria instantânea, telefonia via Internet, redes ponto-a-ponto, videoconferências, redes sociais, etc) com maior grau de especificidade por usuário.

2. Requisitos de Capacitação

1. Trata-se do serviço de treinamento da solução, na modalidade de fornecimento de voucher para treinamento, cujo escopo cubra conceitos de configuração,

operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução de forma que os participantes capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente.

1. O treinamento deverá oferecer carga horária total de no mínimo 20 (vinte) horas.

2. Serão aceitos apenas treinamentos nas modalidades online ao vivo (EAD), podendo as aulas serem gravadas, a critério da CONTRATANTE.

3. A CONTRATADA deverá prover capacitação técnica em turma com no mínimo 1 (um) e no máximo 8 (oito) participantes.

4. O treinamento deverá respeitar o limite de 4 (quatro) horas por dia.

5. O treinamento deverá cobrir conhecimentos necessários para instalação, administração, configuração, gerência, otimização, resolução de problemas e utilização da solução.

2. As despesas decorrentes do serviço de treinamento (instrutores, confecção do material didático, licenciamento de plataforma de videoconferência etc.) serão de exclusiva responsabilidade da CONTRATADA .

3. O treinamento poderá ser composto de mais de 01 (um) módulo, que deverão ser discriminados na proposta da licitante.

4. A licitante deverá anexar a grade de treinamentos do fabricante, com a ementa do(s) curso(s), para comprovar que o(s) treinamento(s) ofertado(s) atende(m) os requisitos indicados nos itens anteriores.

5. O Tribunal poderá planejar e escolher qualquer das datas, ou períodos, dos eventos de capacitação no prazo de validade do Contrato, a contar da entrega do calendário.

6. O treinamento deverá ser ministrado em data oportuna a ser informada à fiscalização antes ou após a instalação da solução, ficando a critério da administração e baseando-se no calendário a ser fornecido pela CONTRATADA .

7. É permitido à CONTRATADA terceirizar o treinamento a outra que preste serviços de treinamento da solução ofertada, ou ao próprio fabricante, desde que mantidas as demais condições deste documento e permanecendo ela a única responsável pelo atendimento do Contrato para todos os fins.

8. O treinamento deverá ser ministrado por profissionais certificados pelo fabricante (com a certificação mais alta do fabricante), cuja comprovação deverá ser encaminhada na assinatura do Contrato.

9. A CONTRATADA deverá fornecer material didático individual, na modalidade digital, que abranja todo o conteúdo do(s) curso(s). Todo o material didático oferecido pela CONTRATADA para realização do treinamento deverá estar atualizado e poderá estar em inglês ou português.

10. O treinamento deverá ser ministrado em português do Brasil. Caso não exista material oficial do produto em língua portuguesa, será aceito material em inglês.

11. O treinamento deverá oferecer acesso a laboratório prático virtual, fornecido pela

CONTRATADA , para configuração e execução de exercícios práticos.

1. No ambiente de treinamento, os participantes indicados pela CONTRATANTE deverão ter acesso em ambiente de laboratório a todos os produtos ofertados (ou similares) para realização da capacitação.

12. A CONTRATADA deverá emitir para o servidor participante, sem ônus para o Tribunal e no prazo máximo de até 10 (dez) dias úteis após o término do treinamento, o certificado de conclusão, no qual deverá constar o nome do treinando, a data, o local e a carga horária. A cópia deste certificado deverá acompanhar a nota fiscal/fatura para o devido pagamento.

13. A ausência do servidor ao treinamento é de responsabilidade do Tribunal, cabendo a CONTRATADA informar no certificado a carga horária e assiduidade do servidor.

3. **Requisitos Legais**

1. O presente processo de contratação deve estar aderente à Constituição Federal, à Lei nº 14.133/2021, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), Resolução TSE Nº 23.644/2021 (Política de Segurança da Informação no âmbito da Justiça Eleitoral) e a outras legislações aplicáveis;

4. **Requisitos de Manutenção**

1. Devido às características da solução, há necessidade de realização de manutenções (corretivas/preventivas/adaptativa/evolutiva) pela CONTRATADA , visando à manutenção da disponibilidade da solução;

2. A CONTRATADA deverá fornecer garantia técnica de pelo menos 36 (trinta e seis) meses para a solução, contados a partir da data de emissão do Termo de Recebimento Definitivo relativo à fase de instalação;

3. Os serviços de garantia técnica englobam todos os elementos de hardware e software da solução, incluindo a prestação de serviços de suporte técnico, assistência corretiva e atualização tecnológica, compreendendo a substituição de peças, componentes, acessórios e aplicativos que apresentem defeito, ou precisem ser atualizados durante este período, sem qualquer ônus adicional para a CONTRATANTE, obrigando-se a CONTRATADA a manter os appliances e aplicativos permanentemente em perfeitas condições de funcionamento para a finalidade a que se destinam;

4. A garantia técnica compreenderá todas as funcionalidades da solução ofertada, tanto as descritas no Termo de Referência quanto as contempladas nos manuais e demais documentos técnicos, incluindo a atualização de versões de software;

5. Qualquer software ou equipamento com hardware defeituoso, peças quebradas, com defeito ou gastas pelo uso normal deverá ser substituído por outro de mesma marca e modelo e com as mesmas características técnicas ou superiores, novo e de primeiro uso, no prazo de 07 (sete) dias úteis a partir de notificação da CONTRATANTE;

6. A CONTRATADA deverá apresentar no protocolo da CONTRATANTE, antes do início da vigência do serviço de garantia técnica, todos os dados necessários

para o registro de chamados técnicos na Central de Atendimento da CONTRATADA , tais como, e-mail, números de telefone e fax, etc;

7. Suporte Técnico durante o período de Garantia Técnica:

    1. Durante o período de garantia técnica de 36 (trinta e seis) meses, a partir do recebimento definitivo da instalação, a CONTRATADA deverá garantir o funcionamento de toda a solução, fornecer atualizações, prestar suporte técnico e atender aos chamados técnicos para manutenção;

    2. A CONTRATADA deverá comunicar formalmente ao Gestor do Contrato a disponibilidade de novas versões e releases das licenças de software e firmwares, reservando-se, à equipe técnica da CONTRATANTE, o direito de exigir a atualização sem que isso implique acréscimo aos preços CONTRATADOs;

    3. A manutenção corretiva será realizada em período integral, 7 (sete) dias por semana e 24 (vinte e quatro) horas por dia, após solicitação da CONTRATANTE;

8. A CONTRATADA deverá entregar no protocolo da CONTRATANTE, mensalmente, até o 5° (quinto) dia útil do mês subsequente, para fins de controle, Relatório Gerencial dos Serviços (RGS) realizado no mês anterior. Deverão constar, no mínimo, as seguintes informações:

    1. Relação de todos os chamados técnicos ocorridos no mês anterior, incluindo data e hora do início e término do suporte; identificação do problema; criticidades; providências adotadas para o diagnóstico, solução provisória e solução definitiva; data e hora do início e término da solução definitiva; identificação do técnico da CONTRATANTE que solicitou e validou o chamado; identificação do técnico da CONTRATADA responsável pela execução do chamado, bem como outras informações pertinentes;

    2. Cada chamado técnico aberto será avaliado individualmente pelo Gestor do Contrato;

    3. O serviço será considerado recebido pelo Gestor do Contrato quando do fechamento de cada chamado, desde que não reapareçam posteriormente ao fechamento inconformidades técnicas comprovadamente relacionadas ao chamado recebido;

    4. O Gestor do Contrato emitirá a recusa em caso de verificação de impropriedades ou erros impeditivos de recebimento do serviço prestado. A CONTRATADA deverá promover as correções necessárias, conforme diretrizes a serem estabelecidas pelo Gestor do Contrato, sem prejuízo de aplicação de penalidades previstas.

9. A CONTRATADA deverá fornecer versão atualizada do manual e demais documentos técnicos sempre que houver atualização nos manuais, nos softwares ou nos appliances da solução;

10. A CONTRATANTE poderá realizar a aplicação de pacotes de correção e migração de versões e releases das licenças de software, quando lhe for conveniente, cabendo à CONTRATADA orientar e colocar à disposição um técnico para contato em caso de dúvidas ou falhas. A CONTRATANTE reserva-se o direito de proceder a outras configurações, instalações ou conexões nos

appliances, desde que tal iniciativa não implique em danos físicos e lógicos aos appliances, sem que isto possa ser usado como pretexto pela CONTRATADA para se desobrigar do suporte da solução;

11. A CONTRATADA deverá garantir pleno funcionamento dos appliances e softwares, bem como atualizações, responsabilizando-se por qualquer componente adicional que for identificado após a contratação, seja por motivos de interoperabilidade, compatibilidade ou quaisquer outros motivos que impeçam o funcionamento efetivo da solução CONTRATADA ;

12. A CONTRATADA deverá dispor de serviço de esclarecimento de dúvidas relativas à utilização dos appliances e de abertura de chamado técnico por e-mail ou por telefone 0800 (gratuito), ou telefone local por todo o período da garantia técnica;

13. A CONTRATADA deverá garantir, sem quaisquer custos adicionais, as atualizações havidas nos appliances nas versões de software e firmware, inclusive releases, pelo prazo de vigência da garantia;

14. O serviço de garantia técnica deverá permitir o acesso da CONTRATANTE à base de dados de conhecimento do fabricante dos appliances, provendo informações, assistência e orientação para diagnósticos, avaliações e resolução de problemas, características dos produtos e demais atividades relacionadas à correta operação e funcionamento dos mesmos;

15. As atualizações e correções (patches) do software e firmwares deverão estar disponibilizados via WEB ou fornecidas em mídia (CD ou DVD), quando desta forma forem solicitadas;

16. Quando a garantia técnica for acionada, o atendimento deverá ser iniciado imediatamente, independente do meio utilizado. A cada abertura de chamado, a CONTRATADA deverá fornecer ao CONTRATANTE um código identificador único para acompanhamento;

17. A CONTRATADA deverá conceder acesso ao CONTRATANTE ao controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do Gestor do Contrato.

5. **Requisitos Temporais**

    1. A Entrega dos equipamentos deverá ser efetivada no prazo máximo de 90 (noventa) dias corridos, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela CONTRATANTE, podendo ser prorrogada, excepcionalmente, por até igual período, desde que justificado previamente pela CONTRATADA e autorizado pela CONTRATANTE;

    2. Deverá ser realizada, após a assinatura do Contrato, uma reunião de alinhamento remota, com o objetivo de alinhar as expectativas, nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e em seus Anexos, e esclarecer possíveis dúvidas acerca do objeto, conforme agendamento efetuado pelo Gestor do Contrato, bem como:

        1. Apresentar a relação do pessoal técnico especializado, adequado e disponível para a execução do objeto deste Estudo, bem como a qualificação de cada um dos membros da equipe técnica.

2. Apresentar a declaração de disponibilidade, assinada por cada integrante da equipe técnica mencionada na alínea anterior, bem como o Termo de Confidencialidade da Informação.

3. Apresentar um cronograma para implantação e configuração da Solução adquirida, o qual deverá sofrer aval do Gestor do Contrato.

4. Apresentar a logística para realização do treinamento da Solução adquirida.

5. Os profissionais indicados pela CONTRATADA deverão efetivamente implantar e configurar a Solução objeto deste Estudo, admitindo-se suas substituições por profissionais de experiência equivalente ou superior, desde que aprovada previamente pelo órgão.

6. O prazo de implantação, instalação e configuração da solução será de até 30 (trinta) dias consecutivos a partir do recebimento do objeto.

6. **Requisitos de Segurança e Privacidade**

1. CONTRATADA deverá submeter-se aos procedimentos de segurança existentes, ou que possam ser criados durante a vigência do Contrato. Os procedimentos deverão ser observados sempre que for necessária a presença nas dependências da CONTRATANTE.

2. A CONTRATADA deverá respeitar as diretrizes constantes da Política de Segurança da Informação (PSI) no âmbito da Justiça Eleitoral (Resolução TSE Nº 23.644/2021), obrigando-se a manter sigilo a respeito de quaisquer informações, dados, processos, fórmulas, códigos, cadastros, fluxogramas, diagramas lógicos, dispositivos, modelos ou outros materiais de propriedade do Tribunal Regional Eleitoral do Piauí, e de outros partícipes desta contratação, aos quais tiver acesso em decorrência do objeto da presente contratação, ficando terminantemente proibida de fazer uso ou revelação destes sob qualquer justificativa.

3. O Tribunal Regional Eleitoral do Piauí terá propriedade sobre todos os documentos e procedimentos operacionais produzidos no escopo da presente contratação.

4. Os documentos eventualmente produzidos deverão ser repassados ao Tribunal tanto em formato não editável (PDF) como também em formato editável (.DOCX).

5. O fornecedor assinará, no ato da entrega das licenças e do serviço, Termo de Confidencialidade, em que se comprometerá a não acessar, não divulgar e a proteger todos os dados de infraestrutura e de vulnerabilidades da CONTRATANTE a que tiver acesso, que abrangerá todos os seus colaboradores e terceiros, sob as penas da lei.

7. **Requisitos Sociais, Ambientais e Culturais**

1. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:

1. A documentação e os manuais da solução deverão, preferencialmente, ser apresentados no idioma Português (Brasil), eventualmente poderão ser apresentados em inglês. Todos os contatos para gerenciamento de chamados e suporte técnico deverão ser realizados em Português (Brasil).

2. O licenciamento e o suporte deverão ser prestados preferencialmente no idioma português do Brasil.

3. Os softwares aplicativos e interface do software deverão ter a possibilidade de escolha de idioma pelo usuário. Será admitido o idioma inglês somente quando não existir uma versão no idioma português do Brasil.

4. Os profissionais da CONTRATADA deverão trajar-se de maneira respeitável e usar linguagem respeitosa e formal no trato com os servidores do órgão, Gestão Contratual e os dirigentes da CONTRATANTE.

8. **Requisitos da Arquitetura Tecnológica**

    1. Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos a seguir:

        1. **Desempenho, Capacidade e Alta Disponibilidade:**

            1. A solução de Secure Web Gateway deverá ser de arquitetura de 64 bits dedicada para este fim, isto é, do tipo "appliance" físico ou virtual, instalado e configurado para fazer o tratamento do tráfego de dados dentro da infraestrutura pertencente a este Tribunal Regional Eleitoral do Píauí, não podendo ser servidor de uso genérico;

            2. Não serão aceitos soluções do tipo SaaS ("Software as a Service") que façam o envio para tratamento no tráfigo de dados em nuvem privada fora da infraestrutura pertencente a este Tribunal Regional Eleitoral do Piauí.

            3. A solução deverá prover toda infraestrutura de hardware e software necessária para seu pleno funcionamento, o que inclui armazenamento de logs, relatórios resumidos ou detalhados, gerenciamento e qualquer outro que se faça necessário, respeitando os requisitos mínimos de hardware do fabricante, itens de suporte e garantia presentes neste edital;

            4. Caso a solução oferecida seja do tipo "aplliance virtual", deverá ser devidamente compatível e homologada com as plataformas de virtualização: VMWare ESX (vSphere 7 ou superior) e Microsoft Hyper-V (Windows Server 2012 R2);

            5. Caso a solução oferecida seja do tipo "aplliance físico", deverá ser fornecido com:

                1. No mínimo 05 (cinco) interfaces 10/100/1000BaseT, sendo uma destas dedicada ao gerenciamento da solução;

                2. Fonte de alimentação elétrica redundante e hot swappable, com chaveamento automático e capacidade de operar nas tensões de 100 a 240 V, 50 – 60Hz. A fonte fornecida deverá suportar sozinha a operação da unidade com todos os módulos de interface ativos. Não serão aceitas fontes redundantes externas ao equipamento;

                3. Cabos elétricos com conector padrão 2P+T, e quaisquer acessórios necessários para interligação do equipamento à rede

elétrica do TRE-PI. A necessidade de qualquer mudança nas tomadas (plugs) para adequação à rede elétrica será de responsabilidade da CONTRATADA , a qual deverá assegurar a manutenção e garantia dos appliances fornecidos;

4. Unidade de armazenamento de, no mínimo, 1TB;

5. Suporte a montagem em Rack de 19”;

6. O hardware da solução deverá ser dimensionado para suportar a capacidade descrita neste edital, com utilização máxima de 80% em seu processamento.

6. A solução deverá prover as funcionalidades de Proxy HTTP/HTTPS, Filtro de Conteúdo, Caching e AntiMalware, incluindo e inspeção de tráfego SSL e Monitoramento de camada quatro do modelo OSI;

7. Todas as funcionalidades especificadas dos appliances deverão estar aptas e licenciadas no ato de sua aquisição, sem custos adicionais para sua plena utilização; caso ocorra a necessidade de instalação de Patch’s e atualização, os mesmos não poderão afetar as funcionalidades exigidas neste edital;

8. O software deverá prever atualizações, incluindo melhorias e novas versões durante o período de vigência do contrato de suporte;

9. A solução deverá possuir sistema de licenciamento modular, no sentido de permitir ativação de funcionalidades mediante futura aquisição e aplicação de licença específica, sem necessidade de adição ou instalação de módulos adicionais de hardware e software;

10. Todas as interfaces fornecidas nos appliances devem estar completamente licenciadas e habilitadas para uso imediato;

11. Cada appliance físico ou virtual deverá suportar, no mínimo, quatro conexões com a Internet, sendo duas conexões para DMZ e duas conexões para rede interna, todas com possibilidade de agregação de links. As portas mencionadas deverão permitir seu uso para qualquer função a critério deste TRE-PI conforme sua necessidade sem que as mesmas sejam específicas e dedicadas para redes internas, externas ou DMZ;

12. Deverá possuri a funcionalidade de Proxy Web, suportando os protocolos HTTP, HTTPS e FTP, em seus modos ativo e passivo;

13. Deverá ser capaz de atuar como um proxy explícito e transparente;

14. Deverá suporta o protocolo ICAP para integração com outras soluções de segurança, como por exemplo DLP (Data Loss Prevention);

15. Deverá suportar integração com múltiplos servidores via ICAP, para tolerância à falhas e balanceamento de carga;

16. Deverá ser compatível com todos os navegadores Web (“browsers”) e sistemas operacionais padrões de mercado;

17. Deverá ser licenciado para suportar uma base de Active Directory

com a quantidade de 1.500 de usuários totais;

18. Deverá ser capaz de suportar navegação de internet típica de 1000 usuários simultâneos, com aferição deste valor em tempo real, identificação de usuários, controle de acesso à Internet (controle de aplicações e filtragem de URL's), administração de largura de banda de serviço de Internet (Traffic Shapping), decriptografia e inspeção de tráfego SSL.

19. A solução deverá ser dimensionada para analisar e filtrar tráfego de, no mínimo, 400Mbps, considerando HTTP e HTTPS;

20. O equipamento oferecido deverá permitir o adicionamento de licenças para até 1.500 usuários sem a necessidade de upgrades físicos;

21. Deverá ser composta por dois appliances em cluster Ativo-Ativo e Ativo-Passivo com processamento e alimentação individual, de maneira que, caso ocorra uma parada ou defeito parcial de um dos appliances, isso não interfira de modo algum no funcionamento da solução, sendo um dos nós capaz de suportar a capacidade total exigida para a solução, bem como licenciamento;

22. Caso o appliance físico não execute a função de gerenciamento unificado e emissão de relatórios, será admitido o gerenciamento unificado através de appliance virtual compatível com o ambiente virtualizado do TRE-PI, a saber: VMWare ESX (vSphere 7 ou superior);

23. A solução deverá permitir a configuração manual e automática de horário através de uso NTP ou SNTP;

24. Deverá possuir suporte a implementação e compatibilidade com os protocolos IPv4 e IPv6;

25. HA (*High availability*) em appliances distintos, suportando topologias ativo-passivo e ativo-ativo, de forma a permitir alta disponibilidade de site. Por alta disponibilidade entende-se que um único appliance deverá ser capaz de sustentar a todos os requisitos da presente documentação sem perda de performance.

2. **Gerenciamento:**

    1. Deverá possuir solução de gerenciamento e administração centralizada capaz de gerenciar e administrar todos os equipamentos envolvidos na solução, desde que não sejam software livre;

    2. Deverá estar equipado com recurso que assegure o gerenciamento remoto através de web browser com suporte a SSL;

    3. Deverá possuir recurso que assegure a atualização e correção de versões de software dos appliances de forma remota e através de interface gráfica;

    4. Deverá possuir capacidade de integração com Serviços de Domínio Active Directory Windows (AD DS), possibilitando o gerenciamento e administração da ferramenta com base nas informações deste serviço;

5. A autenticação deverá ser baseada em ao menos dois dos quatro seguintes protocolos: NTLM, Kerberos, Ldap, Radius.

6. A autenticação deverá ocorrer de modo transparente, utilizando usuário já autenticado em domínio Windows sem pedir novamente a senha de acesso (Single Sign-On);

7. A autenticação de usuários e estações de trabalho deverá ocorrer sem a necessidade de instalação ou execução de clientes ou quaisquer módulos em nenhuma estação de trabalho ou servidor;

8. A capacidade para gerência e administração da ferramenta deverá possibilitar a concessão de direitos a usuários e grupos com no mínimo três níveis de privilégios, como por exemplo: Administrador, operação e emissor de relatórios;

9. Todas as operações da solução deverão ser executadas em console único, e somente será admitida a necessidade de acesso a outros consoles para tarefas de manutenção da ferramenta e troubleshooting (resolução de problemas);

10. A interface de gerenciamento e relatórios suportar autenticação "two-factor" para garantir maior segurança no acesso ao sistema.

11. Deverá possuir gerenciamento do equipamento via protocolo SSH e gráfico (web) via protocolo HTTP ou HTTPS de forma intuitiva e amigável (point-and-click), possibilitando todo gerenciamento, tais como criação de políticas, resolução de problema e acesso a relatórios, sem a necessidade da CLI (Command Line Interface) ou semelhante, como, por exemplo, CLI HTTP;

12. Deverá possuir auditoria de configuração, gravando e disponibilizando todas as alterações que identifique, no mínimo, quem, quando e o que foi alterado;

13. Deverá permitir a execução de cópias de segurança (backup) de forma manual e automática, e permitir também a restauração destas cópias;

14. Deverá implementar os padrões abertos de gerência de rede SNMPv2c e SNMPv3, incluindo a geração de traps.

15. Caso a solução possua licenças relacionadas a capacidade de log indexados e armazenamento, deverá ser ofertado a maior capacidade suportada ou ilimitada;

16. Caso a solução possua módulo de relatórios estendida, deverá ser entregue junto com a solução;

17. O gerenciamento da solução deverá possibilitar a coleta de estatísticas de todo o tráfego que passar pelos equipamentos da plataforma de segurança;

18. Deverá centralizar a administração de regras e políticas dos equipamentos de proteção de rede, usando uma única interface de gerenciamento;

19. Todos os logs da solução devem ser indexados e seu licenciamento deverá ser o de maior capacidade;

20. O gerenciamento deverá permitir/possuir monitoração de logs, ferramentas de investigação de logs e acesso concorrente de administradores;

21. Deverá possuir mecanismo de busca por comandos no gerenciamento via SSH, facilitando a localização de comandos;

22. Suportar criação de regras que fiquem ativas em horário definido e suportar criação de regras com data de expiração;

23. Deverá possuir recurso que assegure o backup da configuração dos appliances, bem como o retorno da configuração utilizando um backup realizado anteriormente, sem a necessidade de se reinicializar o sistema;

24. Suportar validação de regras antes da aplicação;

25. Deverá permitir a visualização dos logs de uma regra específica em tempo real;

26. Deverá possibilitar a integração com outras soluções de SIEM de mercado desde que não sejam software livre;

27. Deverá suportar geração de logs de auditoria detalhados, informando a configuração realizada, o administrador que a realizou e o horário da alteração;

28. Deverá suportar Autoridade Certificadora Interna e Externa (de terceiros) para inspeção do tráfego SSL;

29. Deverá permitir o login de multiplos usuários administradores simultaneos com perfil de escrita, possibilitando agilidade e rapidez no gerenciamento pelo grupo de administradores da solução;

30. Deverá possuir logs, correlação de eventos e relatórios de auditoria dos administradores da solução;

31. Deverá prover uma visualização sumarizada de todas as aplicações, ameaças (Antivírus, Anti-Malware), e URLs que passaram pela solução;

32. Deverá ser possível exportar os logs em CSV ou TXT;

33. Deverá possibilitar rotação do log;

34. O gerenciamento centralizado poderá ser entregue como appliance virtual e deverá ser compatível e homologado para ambiente VMWare ESX vSphere 7 ou superiror;

35. Deverá possuir capacidade de integração com soluções de terceiros via API e também suportar configurações através de RestAPI;

36. Deverá consolidar logs e relatórios de todos os dispositivos administrados;

37. Deverá possuir capacidade de definir administradores com diferentes perfis de acesso com, no mínimo, as permissões de Leitura/Escrita e somente Leitura;

38. Deverá possuir mecanismo de Drill-Down para navegação e análise dos logs em tempo real;

39. Nas opções de Drill-Down, deverá ser possível identificar o usuário que fez determinado acesso;

40. Deverá permitir a customização do padrão regulatório da própria instituição;

41. Deverá permitir notificação instantânea sobre mudanças de política de segurança que impactam negativamente a segurança;

42. Deverá monitorar constantemente o status de conformidade da solução aos padrões regulatórios informados;

43. Deverá destacar potenciais violações de segurança e conformidade, reduzindo o tempo necessário e os erros associados a gestão de conformidade manual;

44. Deverá gerar alertas de conformidade, notificando os usuários sobre o impacto de suas decisões de segurança, trazendo as considerações regulatórias na gestão de segurança;

45. Deverá permitir o gerenciamento eficaz das ações e recomendações, facilitando a priorização e programação de itens de ação;

46. Deverá possuir alertas de políticas e as potenciais violações de conformidade;

47. Deverá possuir recomendações de segurança acionáveis e orientações sobre como melhorar a segurança;

48. Deverá permitir a criação de filtros com base em qualquer característica do evento, tais como a origem e o IP destino, serviço, tipo de evento, severidade do evento, nome do ataque, o país de origem e destino, etc;

49. Deverá prover, no mínimo, as seguintes funcionalidade para análise avançada dos incidentes:

    1. Visualizar quantidade de tráfego utilizado de aplicações e navegação;

    2. Gráficos com principais eventos de segurança de acordo com a funcionalidade selecionada;

50. A solução deverá ser capaz de detectar ataques de tentativa de login e senha utilizando tipos diferentes de credencias;

51. A plataforma de gerência e monitoramento centralizada deverá possibilitar a visualização dos logs de navegação web a partir de um único local, possibilitando a procura correlacionada de logs em uma única tela;

52. A plataforma de gerência centralizada e monitoração deverá possibilitar a procura por IPs e redes, sendo que os resultados mostrem estes IPs e redes nos campos de origem e destino do logs na mesma tela de pesquisa;

53. Deverá possuir mecanismo para que logs antigos sejam removidos automaticamente;

54. Deverá possuir a capacidade de personalização de gráficos como barra, linha e tabela;

55. Deverá permitir a criação de dashboards customizados para visibilidades do tráfego de aplicativos, categorias de URL, ameaças, serviços, países, origem e destino;

56. Deverá possuir a capacidade de visualizar na interface gráfica da solução, informações do sistema como licenças, memória, disco e uso de CPU;

57. Deverá ser capaz de correlacionar eventos de todas as fontes de log em tempo real;

58. Deverá fornecer conteúdo de correlação pré-definido organizado por categoria;

59. Deverá ser capaz de personalizar e criar regras de correlação;

60. Deverá fornecer uma interface gráfica para criação das regras citadas no item anterior;

61. Deverá possuir painéis de eventos em tempo real com possibilidade de configuração das atualizações e frequências;

3. **Controle de Aplicações:**

    1. Deverá permitir a criação de regras que possibilite a permissão ou bloqueio de aplicações diversas, tais como:

        1. Protocolos de banco de dados:

        2. Protocolos de transferência de arquivos;

        3. Protocolos de mensagem instantâneas e bate-papos;

        4. Protocolos de email e ferramentas de colaboração;

        5. Protocolos de compartilhamento de arquivos ponto-a-ponto;

        6. Protocolos de evitação de proxy;

        7. Protocolos de acesso remoto;

        8. Protocolos de streaming de media;

        9. Protocolos de sistema operacional de rede.

    2. Deverá possuir recurso para classificar aplicações Web 2.0, entre elas: “Facebook”, “LinkedIn”, “Twitter”, e “Youtube”,. Esta

característica da Solução deve ser baseada em assinaturas recebidas automaticamente pelo fabricante;

3. Deverá possuir recurso para classificar aplicações nuvem. Esta característica da Solução deve ser baseada em assinaturas recebidas automaticamente pelo fabricante;

4. Deverá permitir controle de políticas por aplicações, grupos de aplicações e categorias de aplicações;

5. Deverá permitir controle de políticas por usuários, grupos de usuários, IPs e redes;

6. Deverá decriptografar tráfego de entrada e saída em conexões negociadas com TLS 1.2;

7. Deverá ser capaz de decodificar e detectar códigos maliciosos dentro de aplicações RIA (como Flash, Adobe AIR, Silverlight, entre outros);

8. Deverá possuir recurso para detectar automaticamente protocolos de streaming encapsulados em HTTP e tratá-los como protocolos nativos;

9. Será aceito soluções de outros fabricantes diferentes da solução de segurança ofertada pela licitante desde que atendido todos os requisitos desta especificação;

10. Deverá suportar a atribuição de agendamento às políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente;

11. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo, com as seguintes funcionalidades:

    1. Deverá ser possível a liberação e bloqueio de aplicações sem a necessidade de liberação de portas e protocolos;

    2. Deverá reconhecer pelo menos 6.000 (seis mil) aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;

    3. A checagem de assinaturas deverá determinar se uma aplicação está utilizando a porta padrão ou não;

    4. Para inspeção SSL, ou HTTPS Inspection, a solução deve oferecer suporte ao Perfect Forward Secrecy (conjuntos de cifras PFS, ECDHE);

    5. Para tráfego criptografado (SSL), deve decriptografar pacotes a fim de possibilitar a leitura do payload para checagem de assinaturas de aplicações conhecidas;

12. Deverá realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o

tráfego corresponde com a especificação do protocolo;

13. Deverá permitir a configuração de categorias ou sites isolados para que o tráfego SSL não seja decriptado;

14. Deverá possuir pelo menos 90 categorias de aplicações WEB pré-definidas pelo fabricante;

15. Para solução de filtro de conteúdo e controle web, deverá ser capaz de bloquear na mesma aplicação um conteúdo específico sem bloquear a aplicação principal (Ex.: Whatsapp Web, Whatsapp voice e Whatsapp file transfer.);

16. Deverá possuir mecanismo de controle de aplicação web e URL que possibilite a configuração de bloqueio e liberação da aplicação principal e/ou as suas sub-categorias, por exemplo, quando o administrador da solução desejar bloquear apenas as sub-categorias do facebook, como facebook chat, video, game, compartilhamento de arquivos ou outros. Ou seja, não deverá ser bloqueado toda a categoria como “Facebook” ou "Redes sociais" que também possa implicar o bloqueio não só do Facebook, mas também de tudo que estiver relacionado às redes sociais, como LinkedIn, Twitter, YouTube, etc.

17. A solução deverá ser baseada em bloqueio de aplicações WEB que a própria base possui, assim a inspeção ocorrerá em camada 7 analisando o payload do pacote;

18. A decodificação de protocolo deve também identificar comportamentos específicos dentro da aplicação;

19. Deverá atualizar a base de assinaturas de aplicações automaticamente;

20. Deverá limitar a banda (download/upload) usada por aplicações, baseado no IP de origem, usuários e grupos do LDAP/AD;

21. Os dispositivos de proteção de rede devem possuir a capacidade de identificar de forma transparente o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no controlador de domínio, nem nas estações dos usuários, permitindo a criação de políticas de segurança baseadas nas informações coletadas, entre elas usuários, IP, grupos de usuários do sistema do Active Directory;

22. Deverá suportar múltiplos métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas, decodificação de protocolos ou análise heurística;

23. Deverá permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias, sem a necessidade de ação do fabricante, mantendo a confidencialidade das aplicações da Instituição;

24. Deverá possibilitar que o controle de portas seja aplicado para todas as aplicações;

25. A plataforma de segurança deve possuir as seguintes funcionalidades de filtro de URL:

    1. Deverá permitir especificar política por tempo, com definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

    2. Deverá ser possível a criação de políticas por Usuários, Grupos de Usuários, IPs e Redes;

    3. Deverá incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs atráves da integração com serviços de diretório, autenticação via Active Directory e base de dados local;

    4. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e Categoria de URL;

    5. Deverá suportar armazenamento, na própria solução, de URLs, evitando delay de comunicação/validação das URLs;

    6. Deverá bloquear o acesso a sites com conteúdo indevido ao utilizar a busca em sites como Google, Bing e Yahoo, mesmo que a opção “Safe Search” esteja desabilitada no navegador do usuário;

    7. Deverá suportar base ou cache de URLs local no appliance, evitando atrasos de comunicação e validação das URLs. Caso a solução ofertada não suporte localmente, será aceito produto externo desde que não seja solução de software livre;

    8. Deverá suportar a criação de categorias de URLs customizadas;

    9. Deverá suportar a exclusão de URLs do bloqueio, por categoria;

26. Deverá permitir a customização de página de bloqueio;

27. Deverá possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, sem a necessidade de instalar nenhum cliente nos servidores Active Directory ou em outra máquina da rede;

28. Deverá permitir o controle, sem instalação de cliente de software, em máquinas/computadores que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente na solução de segurança ofertada (Captive Portal);

4. **Filtro de Acesso:**

    1. Deverá permitir a criação de regras que possibilite a permissão ou bloqueio de acesso baseado nos seguintes critérios:

        1. Origem (Grupos do domínio ou serviço de diretórios LDAP e AD ao qual o usuário pertence; Aplicação);

        2. Destino (Categoria, domínio, url/lista);

3. Tipo de arquivo;

4. Protocolos (HTTPS, FTP e outros);

5. Horário (definir períodos de funcionamento por regra);

2. Deverá permitir definição de largura ou porcentagem de banda máxima para o acesso de acordo com o estabelecido em regra, baseando-se em categoria do destino ou protocolo;

3. A solução deverá atuar como “man in the middle”, intermediando e repassando todas as requisições, permitindo a emissão de certificados auto-assinados ou importados de uma “Certificate Authority” confiável.

4. Deverá permitir a emissão de páginas amigáveis e customizáveis de erro também aos sites criptografados;

5. Deverá possuir funcionalidade de prevenção de acesso a sites HTTPS com certificados expirados ou desconhecidos, permitindo a importação de novas “Certificate Authority” através da interface de gerenciamento;

6. Deverá permitir o controle de acesso através do percentual de largura de banda disponível para determinadas Categorias e os limites de banda deverão ser definidos por:

    1. Limite de Banda ou percentual de Banda - Definindo um limite global para todos os usuários da rede para os tipos de aplicativos para definir um limite global de largura de banda para restringir a quantidade de tráfego de rede;

    2. Limite de Banda por Usuário. Definindo um limite individual para cada usuário da rede para os tipos de aplicativos para definir um limite de largura de banda para restringir a quantidade de tráfego de rede;

7. Deverá possuir mecanismo de classificação em tempo real dos sites visitados ou sistema de filtro de reputação que permita estabelecer uma reputação para cada endereço IP dos servidores de destino. A rede de reputação não deverá somente ser baseada em informações de fluxo da própria base de appliances instalados, mas sim em correlações entre outros parâmetros: listas negras de URL, listas brancas de URL, listas de appliances comprometidos, volume global de trafego, histórico dos sites, dados de categorização de URLs e web crawlers;

8. Não serão aceitas categorias pré-estabelecidas como Unrated, Uncategorized e afins, ou seja, é de responsabilidade do appliance categorizar automaticamente sites que não foram categorizados pelo fabricante anteriormente, realizando a análise do conteúdo do site e categorizando o mesmo de forma adequada;

9. Permitir atualização automática da lista de URLs categorizadas via Internet por meio de base proprietária do fabricante do equipamento;

10. Deverá permitir politicas baseadas em tempo (dias da semana, hora

10. Deverá permitir políticas baseadas em tempo (dias da semana, hora do dia) a fim de restringir acesso a horários pré-estipulados (ex.: horário comercial);

11. Deverá possuir mecanismo de segurança que analise em tempo real a presença de conteúdo malicioso nas páginas acessadas.

5. **Filtro de Dados:**

    1. A solução de controle de dados deverá trazer de fábrica vários tipos de arquivos reconhecidos nativamente, permitindo a reconhecimento de pelo menos os seguintes tipos de arquivos:

        1. PCI - credit card numbers;
        2. HIPAA - Medical Records Number - MRN;
        3. International Bank Account Numbers – IBAN;
        4. Source Code – JAVA;
        5. U.S. Social Security Numbers - According to SSA;
        6. Salary Survey Terms;
        7. Viewer File - PDF;
        8. Executable file;
        9. Database file;
        10. Document file;
        11. Presentation file;
        12. Spreadsheet file;

    2. Deverá permitir que as direções do tráfego inspecionado sejam definidas no momento da criação da politica, tais como: "Upload", "Download" e "Download e Upload";

    3. Deverá permir que o usuário receba uma notificação, redirect de uma página web, sempre que um arquivo reconhecido por match em uma regra em uma das categorias acima, seja feito;

    4. Deverá permitir, inspecionar e prevenir vazamentos de arquivos mesmo quando estes estes sendo trafegados pela Web em páginas utilizando o protocolo HTTPS.

6. **Proteção Contra Ameaças Avançadas - Zero Day:**

    1. Deverá garantir que, além das atualizações diárias pré-programadas, novas páginas cujo conteúdo represente riscos à segurança sejam adicionadas automaticamente à lista de URLs imediatamente após haver sido descobertas pelo fabricante da solução, sem necessidade de interação humana, e sem ter que aguardar pelo horário pré-determinado de atualização da base;

2. Deverá enviar automaticamente para o fabricante da solução, sem intervenção humana, informação sobre todas as URLs não-categorizadas que tenham sido acessadas durante o dia pelos funcionários da empresa, para fins de categorização na base de URLs. O fabricante deverá analisar todas as URLs recebidas e adicionar as que forem pertinentes à lista de URLs que será atualizada automaticamente pelo produto no dia seguinte;

3. Deverá permitir a recategorização manual de qualquer página Web segundo as necessidades da empresa, bem como permite que certas páginas possam ser acessadas a qualquer momento mesmo que pertençam a categorias bloqueadas;

4. A solução deverá prover as funcionalidades de inspeção e prevenção de tráfego de entrada de malwares não conhecidos e do tipo APT;

5. Deverá ser capaz de inspecionar e prevenir malware desconhecido em tráfego criptografado SSL;

6. Deverá implementar, identificar e bloquear malwares de dia zero em anexos de e-mail e URL´s conhecidas;

7. Deverá possuir recurso para bloquear “scripts” ativos como ActiveX, Javascript e VBScript;

8. Deverá fornecer a capacidade de emular ataques em diferentes sistemas operacionais, dentre eles: Windows 10 e superiores e Office 2013, 2016 e superiores;

9. A tecnologia de máquina virtual deverá possuir diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas antes de entregar este arquivo para o cliente;

10. Deverá implementar atualização da base de dados de forma automática, permitindo agendamentos diários, dias da semana ou dias do mês assim como o período de cada atualização;

11. A funcionalidade de prevenção de ameaças avançadas deverá ser habilitada e funcionar de forma independente das outras funcionalidades de segurança;

12. Deverá implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deverá inspecionar arquivo PDF acima de 10 Mb;

13. O relatório das emulações deverá conter print screen dos arquivos emulados, assim como todo detalhamento das atividades executadas em filesystem, registros, uso de rede e manipulação de processos e o relatório das emulações deverá ser individualizado para cada SO emulado;

14. Todas as máquinas virtuais (Windows e pacote Office) utilizadas na solução e solicitadas neste edital, devem estar integralmente instaladas e licenciadas, sem a necessidade de intervenções por

parte do administrador do sistema. As atualizações deverão ser providas pelo fabricante;

15. Deverá implementar mecanismo de exceção, permitindo a criação de regras por subrede e endereço IP;

16. Deverá gerenciar, tipos (MIME) ou extensão de arquivos (MP3, AVI, ISO, WMV, EXE, etc);

17. Deverá implementar a emulação, detecção e bloqueio de qualquer malware e/ou código malicioso detectado como desconhecido. A solução deve permitir a análise e bloqueio dos seguintes tipos de arquivos caso tenham malware desconhecido:

    1. pdf, tar, zip, rar, seven-z, exe rtf, csv, scr, xls, xlsx, xlt, xlm, xltx, xlsm, xltm, xlsb, xla, xlam, xll, xlw, ppt, pptx, pps, pptm, potx, potm, ppam, ppsx, ppsm, sldx, sldm, doc, docx, dot, docm, dotx, dotm e gz;

18. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deverá ocorrer em tempo real e o bloqueio deverá ser imediato. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

19. Deverá possibilitar remoção de conteúdo ativo dinâmico como macros, URL's, Java scripts e outros dos arquivos baixados, permitindo o download do arquivo original caso ele não seja malicioso;

20. Deverá permitir a criação de Whitelists baseado no MD5 do arquivo;

21. Para melhor administração da solução, a solução deverá possibilitar as seguintes visualizações a nível de monitoração:

    1. Número de arquivos emulados;

    2. Número de arquivos com malware.

22. A solução de prevenção de ameaças avançada deverá possuir capacidade de apresentar em seus logs visibilidade de acordo com o framework ATT&CK Mitre Matrix, pontuando características de táticas e técnicas de acordo com a ameaça detecada/bloqueada pela solução. Caso a solução não possua determinada capacidade, poderá ser integrada com outras soluções de mercado, não sendo elas soluções abertas;

23. Deverá prover informação, seja por meio de relatório ou log, sobre as seguintes situações:

    1. O tamanho máximo do arquivo emulado seja excedido;

    2. O tempo máximo de emulação seja excedido.

7. **Relatórios:**

    1. O relatório deverá apresentar eventos em um unico portal (dashboard) e geração de relatório de todas as funcionalidades de segurança que estão ativadas nos gateways de segurança;

2. Deverá possuir relatório e telas de apresentação onde conste todos os principais eventos das funcionalidades de controle de aplicação web, filtro URL, prevenção de ameaças (Antivírus, Anti-Malware);

3. Deverá permitir criação de relatórios customizados via interface gráfica, sem necessidade de conhecer linguagens de banco de dados;

4. Deverá possibilitar a geração de relatórios de eventos no formato PDF ou HTML;

5. Deverá suportar geração de relatórios. No mínimo os seguintes relatórios devem ser gerados:

    1. Utilização da Internet por usuário, grupos, categorias, períodos e protocolos;

    2. Navegação detalhada por usuário para categorias permitidas;

    3. Navegação detalhada por usuário para categorias bloqueadas;

    4. Relação de aplicações WEB 2.0 utilizadas pelos usuários;

    5. Visualização do log de acesso completo dos usuários;

    6. Top N de sítios web mais acessados;

    7. Top N categorias mais acessadas;

    8. Top N de usuários mais ativos;

    9. Top N de grupos de usuários mais ativos;

6. Deverá permitir a criação de relatórios personalizados;

7. Deverá gerar relatórios regulamentares com base nas configurações de segurança em tempo real;

8. Deverá permitir que os relatórios possam ser salvos, enviados e impressos;

9. Deverá suportar a geração de relatório gerencial para apresentar os eventos de ataque de forma completamente visual, utilizando para tanto gráficos, consumo de banda utilizado pelos ataques e quantidade de eventos gerados e protegidos;

10. Deverá permitir a geração de painel e relatórios contendo mapas geográficos gerados em tempo real para a visualização das principais ameaças através de origens e destinos do tráfego gerado na Instituição;

11. Deverá possuir recursos que permita com que, a partir de informações como usuário e url, o sistema possa informar se o acesso será permitido ou negado e em que política ele passou ou o porquê foi bloqueado;

12. Deverá possuir capacidade de listar todos os acessos ao proxy,

permitindo a filtragem por, no mínimo, os campos Usuário/Ip/Categoria, exibindo informações como url acessada, categoria, política utilizada no acesso ou bloqueio;

13. Deverá prover um painel gráfico (Dashboard) de ameaças que liste incidentes detectados/bloqueados na rede contendo as seguintes informações sobre cada um:
    1. Nivel de severidade;
    2. Categoria da ameaça;
    3. Nome da ameaça;
    4. Ação aplicada;
    5. Politica aplicada;
    6. Nome do usuário;
    7. IP de origem;
    8. IP de destino;
    9. Porta;
    10. Protocolo;
    11. Metodo;
    12. URL de acesso;
    13. País de origem;
    14. Dados forenses;
    15. User agent.
14. Deverá possuir módulo de relatórios sobre utilização de aplicações em nuvem dos usuários da rede contendo as seguintes informações:
    1. Nome da aplicação em nuvem;
    2. Nivel de Risco que a utilização de tal aplicação representa;
    3. Descritivo do Tipo da Aplicação;
    4. Usuário(s) ou IP(s) que acessaram a aplicação;
    5. Numero de requisições para cada aplicação;
    6. Bytes enviados;
    7. Bytes recebidos.
15. Deverá exibir relatórios de atividades por usuário com os seguintes campos: site acessado, categorias, bloqueados e permitidos, consumo de banda;

16. Deverá emitir relatórios customizáveis, produzindo documentos de múltiplos níveis;

17. Deverá permitir a exportação dos dados dos relatórios para no mínimo dois dos seguintes formatos: CSV, PDF e HTML;

18. Deverá possibilitar o agendamento de geração de relatório periódico e que o relatório seja exportado automaticamente para no mínimo dois destinos: e-mail, compartilhamento, FTP ou SCP.

9. **Requisitos de Implantação**

    1. Os equipamentos deverão observar integralmente os requisitos de implantação, instalação e fornecimento descritos a seguir:

        1. **Implantação, Configuração E Migração:**

            1. A infraestrutura lógica de proxy presente hoje no TRE-PI é composta por:

                1. Proxy Web:

                    1. Responsável por atuar como intermediário entre o cliente e o servidor de destino externo;

                    2. Possui recursos para cache de conteúdo, autenticação de usuários e controle de acesso;

                    3. Utilizado para reduzir a quantidade de tráfego na rede, armazenando em cache solicitações frequentes;

                2. Proxy Reverso Interno:

                    1. Atua como intermediário entre os clientes e os servidores de destino internos;

                    2. É configurado para redirecionar solicitações para servidores específicos, balancear a carga entre vários servidores e proteger o servidor de destino contra ataques;

                3. Proxy Reverso Externo:

                    1. Atua como intermediário entre os clientes e os servidores de destino externos;

                    2. Utilizado para distribuição de carga e melhoria do desempenho dos servidores;

                    3. É configurado para rotear as solicitações de acordo com as configurações definidas pelo administrador;

            2. Deverão ser configurados na solução todos os perfis de acesso via proxy existente na atual infraestrutura, que são compostas por 16 regras de acesso sendo:

                1. 1 Regra de acesso a somente um grupo de sites delimitados;

    2. 4 Regras de acesso para diferentes categorias de acesso à internet;

    3. 1 Regra de acesso por cota de tempo.

3. Deverá ser configurado 5 regras permitindo acesso a ranges de IP de forma anônima para a um grupo de sites da Internet.

4. Na solução atual foi realizada a mudança de categoria a 130 sites localmente, caso estes sites estejam categorizados em categorias diferentes na nova solução, os mesmos deverão ser reconfigurados conforme ambiente atual.

5. Deverá ser configurado 65 protocolos customizados a partir de um ou um grupo de portas.

6. Deverão ser levantadas junto à equipe designada pela CONTRATANTE quais das novas funcionalidades que, embora não existam na solução atual, serão implantadas durante esta migração. Esta lista terá como limite todas as funcionalidades requeridas para o produto neste edital;

7. Deverá ser proposta à equipe designada pela CONTRATANTE, as possíveis topologias (físicas e lógicas) da solução de Proxy de modo que atenda melhor a necessidade do TRE-PI diante do cenário encontrado, estando sujeito à aprovação e aceite da equipe designada da CONTRATANTE;

8. Antes da execução dos serviços de implantação da solução proposta, deverá ser realizada uma reunião com a presença dos arquitetos da solução do fornecedor, os analistas da CONTRATANTE envolvidos no projeto e a equipe do Núcleo de Segurança de TI, para elaboração do plano do projeto para a implantação da solução, de forma a seguir as boas práticas de gerenciamento de projetos, incluindo:

    1. Estudos de viabilidade, configuração, instalação e migração;

    2. Detalhamento das atividades;

    3. Escopo;

    4. Cronograma;

    5. Recursos;

    6. Análise de riscos e impacto;

    7. Plano de contingências;

    8. Marcos do projeto;

    9. Reuniões de acompanhamento, entre outros;

    10. Documentação necessária.

9. Todo o processo de migração da solução para a nova infraestrutura, instalação e configuração dos novos appliances é de

responsabilidade da empresa CONTRATADA , devendo ser realizado por pessoal capacitado, comprovadamente certificado e autorizado pelo fabricante do equipamento adquirido, sob a supervisão da equipe designada da CONTRATANTE, que por sua vez deverão fornecer à empresa CONTRATADA as informações necessárias para tal;

10. A instalação dos appliances adquiridos deve ser feita de forma paralela à infraestrutura atual e a migração para o novo núcleo deve acontecer de forma programada e definida pelos analistas da CONTRATANTE, com o mínimo possível de interrupção do funcionamento da solução atual, devendo toda e qualquer interrupção ser comunicada, programada e autorizada pela CONTRATANTE;

11. Certificação final da solução, mediante testes de comunicação e apresentação de relatórios com os dados gerados. Os testes deverão compreender a comprovação de forma inequívoca do perfeito funcionamento dos mecanismos de alta disponibilidade, sejam eles de enlace físico, switches de acesso, switches core e também seus componentes. Todos estes testes deverão ser realizados com o acompanhamento da equipe de analistas da CONTRATANTE;

12. Documentação As-Built de todo o projeto.

13. O procedimento de implantação, instalação e configuração deve ser realizado em até 30 dias após a entrega dos appliances, que pode ser prorrogado em acordo aprovado pela CONTRATANTE.

2. **Teste De Bancada**

    1. Deverão ser apresentados para o pleno atendimento aos requisitos deste edital e ainda em caráter eliminatório, testes de bancada, onde deverão ser comprovadas de forma prática, todas as características e funcionalidades descritas de cada produto ou serviço deste edital. O teste de bancada deverá ser executado em ambiente de Produção da CONTRATANTE.

    2. Após a energização, instalação e configuração inicial do equipamento, o fornecedor/fabricante terá um prazo de 48 (quarenta e oito) horas para demonstrar as funcionalidades solicitadas.

3. **Modelo De Planilha De Atendimento De Requisito**

    1. O atendimento a todos os itens deve ser comprovado através de documentação oficial do fabricante da solução, que deverá ser anexada à proposta comercial ajustada. A instituição poderá realizar diligência junto ao fabricante para comprovar a autenticidade da documentação. A localização da comprovação na(s) página(s) deverá ser clara e precisa. O não atendimento destes requisitos implicará a desclassificação da proposta:

Item	Documento	Página	Localização

10. **Requisitos de Garatia, Manutenção e Assistência Técnica**

    1. O proponente e o fabricante deverão oferecer suporte técnico em língua portuguesa através de ligação telefônica gratuita do tipo 0800, que deve estar disponível no regime de 24 x 7 x 365 (24 horas por dia, 7 dias na semana e 365 dias no ano);

    2. Os componentes da solução deverão ser fornecidos com garantia e suporte do fabricante de 36 (trinta e seis) meses, que deve estar disponível no regime de 24 x 7 x 365 (24 horas por dia, 7 dias na semana e 365 dias no ano), contados depois da assinatura do Contrato, com atendimento on-site, com substituição do equipamento defeituoso ocorrendo em até no máximo 07 (sete) dias úteis após a abertura do chamado ou comprovação do defeito junto ao proponente/fabricante;

    3. Atualizações de firmware e correções deverão estar disponíveis via Internet, sem custo adicional durante o período de garantia;

    4. Em caso de falhas, fica a cargo do fornecedor o envio do produto substituto, e também é de responsabilidade do fornecedor devolver para o fabricante o produto danificado;

    5. Os chamados de suporte técnico podem ser abertos com o proponente e com o suporte técnico do fabricante a critério da CONTRATANTE;

Nível de Severidade	**Descrição**	**Email**	**On Site**
Alto	Serviço completamente indisponível		02 horas
Médio	Serviço operando parcialmente		04 horas
Baixo	Serviço com degradação de desempenho ou funcionalidade	08 horas	
Normal	Aplicação de patchs, hotfixes e firmware		Agendamento de 48 horas

    6. Os chamados de severidade baixa, ou seja, aqueles que não afetam o desempenho da solução ou funcionalidades que não sejam de suma importância,

deverão possuir um tempo de resposta máximo de 8h (oito horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado por e-mail. Para solução do problema o SLA solicitado será apenas para hardware.

7. Os chamados de severidade média, ou seja, aqueles que influenciam negativamente no funcionamento de alguns dos seus serviços, mas sem torná-la totalmente inoperante, deverão possuir um tempo de resposta máxima de 4h (quatro horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado On-Site. Para solução do problema o SLA solicitado será apenas para hardware.

8. Os chamados de severidade crítica, ou seja, aqueles relacionados a impactos de alta relevância que impedem a operação da solução, deverão possuir um tempo de resposta máximo de 02h (duas horas) para diagnóstico e solução do problema, o mesmo deverá ser realizado On Site. Para solução do problema o SLA solicitado será apenas para hardware.

9. Caberá exclusivamente à CONTRATANTE a categorização do chamado no ato da sua abertura.

10. O prazo de garantia contratual dos bens, complementar à garantia legal, será de, no mínimo, 36 (trinta e seis) meses, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

11. Caso o prazo da garantia oferecida pelo fabricante seja inferior ao estabelecido nesta cláusula, o fornecedor deverá complementar a garantia do bem ofertado pelo período restante.

12. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para a CONTRATANTE.

13. A garantia abrange a realização da manutenção corretiva dos bens pela própria CONTRATADA, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

14. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

15. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

16. Uma vez notificado, a CONTRATADA realizará a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 15 (quinze) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pela CONTRATADA ou pela assistência técnica autorizada.

17. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser prorrogado uma única vez, por igual período, mediante solicitação escrita e justificada da CONTRATADA, aceita pela CONTRATANTE.

18. Na hipótese do subitem acima, a CONTRATADA deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente

fornecido, para utilização em caráter provisório pela CONTRATANTE, de modo a garantir a continuidade dos trabalhos administrativos durante a execução dos reparos.

19. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação da CONTRATANTE ou a apresentação de justificativas pela CONTRATADA, fica a CONTRATANTE autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir da CONTRATADA o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.

20. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade da CONTRATADA.

21. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no Contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.

11. **Requisitos de Experiência Profissional**

    1. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

    2. A implantação deve ser realizada por profissionais certificados, que possuam certificação do fabricante da solução adquirida ou pelo próprio fabricante, que lhes confiram as competências necessárias para a realização dos respectivos serviços.

    3. Para esta solução é necessária a capacitação do corpo técnico e implementação com acompanhamento de um profissional especializado na solução e/ou pelo próprio fabricante, por se tratar de uma solução complexa.

    4. A proponente deverá possuir pelo menos 1 (um) profissional capacitado com certificação, e deverá apresentar certificado técnico da solução durante a fase de habilitação.

    5. Os profissionais que inicialmente manterão relacionamento direto com a CONTRATANTE deverão ser apresentados após assinatura do Contrato na REUNIÃO INICIAL, ocasião em que deverão ser entregues as comprovações dos perfis exigidos. A apresentação de novos profissionais durante a execução do Contrato, incluindo a entrega das comprovações dos perfis à equipe de fiscalização do Contrato, deverá ser feita previamente ao início da atuação destes.

12. **Requisitos de Formação da Equipe**

    1. Os serviços deverão ser prestados por técnicos devidamente capacitados, de acordo com os critérios estabelecidos a seguir:

        1. O profissional que atuará como gerente de projeto deve ter certificação como Project Management Professional (PMP);

        2. A CONTRATADA deverá apresentar profissional(is) com certificação técnica emitida pelo fabricante ou instituto autorizado pelo respectivo

fabricante do Secure Web Gateway, indicando sua habilitação técnica na tecnologia ofertada. Este profissional deve executar “in loco” os serviços especificados e prestar o suporte e o atendimento em garantia dos produtos.

13. **Requisitos de Metodologia de Trabalho**

    1. O fornecimento dos equipamentos está condicionado ao recebimento pela CONTRATADA de Ordem de fornecimento de Bens (OFB) emitida pela CONTRATANTE.

    2. A OFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

    3. O andamento do fornecimento dos equipamentos dever ser acompanhado pela CONTRATADA, que dará ciência de eventuais acontecimentos à CONTRATANTE.

14. **Requisitos de Segurança da Informação e Privacidade**

    1. A CONTRATADA deverá observar integralmente os requisitos de Segurança da Informação e Privacidade elencados na Política de Segurança da Informação do Tribunal Regional Eleitoral do Piauí.

15. **Sustentabilidade**

    1. Além dos critérios de sustentabilidade inseridos na descrição do objeto, devem ser atendidos os requisitos previstos no Guia Nacional de Contratações Sustentáveis e legislação aplicável, a exemplo da IN nº 1, de 19 de janeiro de 2010, da SLTI/MPOG, no que couber.

16. **Da exigência de carta de solidariedade**

    1. Em caso de fornecedor revendedor ou distribuidor, será exigida carta de solidariedade emitida pelo fabricante, que assegure a execução do Contrato.

17. **Subcontratação**

    1. Não é admitida a subcontratação do objeto contratual.

18. **Garantia da Contratação**

    1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

19. **Informações relevantes para o dimensionamento E/OU apresentação da proposta**

    1. A demanda do órgão tem como base as características já expressas no item DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO, onde constam os itens de produtos e serviços e os preços individuais a serem discriminados para a composição do preço global.

5. **PAPÉIS E RESPONSABILIDADES**

    1. São obrigações da CONTRATANTE:

1. Nomear Gestor e Fiscais Técnico, Administrativo e Demandante do Contrato para acompanhar e fiscalizar a execução dos Contratos;

2. Encaminhar formalmente a demanda por meio de Ordem de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis;

5. Liquidar o empenho e efetuar o pagamento à CONTRATADA , dentro dos prazos preestabelecidos em Contrato;

6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

7. Definir produtividade ou capacidade mínima de fornecimento da solução de TIC por parte da CONTRATADA, com base em pesquisas de mercado, quando aplicável;

8. Prever que os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

9. Acompanhar e fiscalizar a execução do fornecimento do objeto contratado, bem como realizar testes nos bens fornecidos de forma a verificar se atendem as especificações e condições exigidas, atestando nas notas fiscais/fatura a efetiva entrega do objeto contratado e o seu aceite;

10. Verificar itens entregues nos quantitativos e versões contratados;

11. Designar responsável para o acompanhamento e fiscalização da execução do objeto contratual;

12. Prestar as informações e os esclarecimentos que venham a ser solicitados pela CONTRATADA ;

2. São obrigações da CONTRATADA:

    1. Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do Contrato;

    2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

    3. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução do Contrato pela CONTRATANTE;

    4. Propiciar todos os meios necessários à fiscalização do Contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento,

total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5. Manter, durante toda a execução do Contrato, as mesmas condições da habilitação;

6. Quando especificada, manter, durante a execução do Contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

7. Quando especificado, manter a produtividade ou a capacidade mínima de fornecimento da solução de TIC durante a execução do Contrato;

8. Ceder os direitos de propriedade intelectual e direitos autorais da solução de TIC sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

9. Fazer a transição contratual, com transferência de conhecimento, tecnologia e técnicas empregadas, sem perda de informações, podendo exigir, inclusive, a capacitação dos técnicos da CONTRATANTE ou da nova empresa que continuará a execução do Contrato, quando for o caso;

6. MODELO DE EXECUÇÃO DO CONTRATO

1. Rotinas de Execução

1. Do Encaminhamento Formal de Demandas

1. A CONTRATANTE emitirá a Ordem de Fornecimento de Bens ou Nota de Empenho para o início dos serviços/entrega dos bens desejados.

2. A CONTRATADA deverá fornecer as licenças de uso com as mesmas configurações e quantidades definidas na Ordem de Fornecimento de Bens ou Nota de Empenho.

3. Os serviços e produtos serão recebidos provisoriamente no prazo de 5 (cinco) dias úteis da data de entrada da respectiva nota fiscal/fatura, pela unidade demandante, para efeito de posterior verificação de sua conformidade com as especificações e quantidades constantes neste Termo de Referência e na proposta/nota fiscal.

4. A verificação técnica e o recebimento definitivo dos serviços e produtos deverão ocorrer no prazo máximo de 10 (dez) dias úteis, contados do primeiro dia útil após a finalização do teste de bancada.

5. O aceite definitivo será efetuado por servidores designados pela Secretaria de Tecnologia da Informação – STI do TRE-PI em conjunto com pelo menos um servidor do setor solicitante da licença.

6. Os serviços prestados e as licenças entregues em desacordo com o especificado neste Termo de Referência e na proposta do fornecedor serão rejeitados parcialmente ou totalmente, conforme o caso, obrigando-se a empresa CONTRATADA a corrigi-los no prazo de 5 (cinco) dias úteis e sem ônus para o TRE-PI, sob pena de ser considerada em atraso quanto ao prazo de entrega.

7. As licenças entregues e os serviços prestados serão inteiramente recusados caso não tenham sido efetuados conforme as especificações técnicas contidas neste Termo de Referência.

2. **Forma de execução e acompanhamento do Contrato**

    1. **Condições de Entrega**

        1. O prazo de entrega dos bens é de 90 (noventa) dias, contados do recebimento da ordem de fornecimento, ordem de serviço ou nota de empenho, em remessa única.

        2. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 10 (dez) dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

        3. Os bens deverão ser entregues no seguinte endereço: Tribunal Regional Eleitoral do Piauí, Praça Edgar Nogueira, 80 - Cabral, Teresina - PI, 64000-920.

        4. Os softwares deverão ser disponibilizados por meio de download, em link direto, próprio, com chave de segurança exclusiva para o Tribunal Regional Eleitoral do Piauí.

3. **Formas de transferência de conhecimento**

    1. A transferência do conhecimento deverá ser realizada observando-se o que segue:

        1. Treinamento ao vivo na modalidade de Ensino a Distância, cujo escopo cubra conceitos de configuração, operação, administração, gerência, otimização, resolução de problemas e gestão de todos os componentes da solução, de forma que os participantes capacitados possam colocar a solução em produção, bem como planejar mudanças de configuração no ambiente.

4. **Procedimentos de transição e finalização do Contrato**

    1. Os procedimentos de transição e finalização do contrato englobam o fornecimento dos dados produzidos em decorrência da relação contratual, à Administração.

5. **Quantidade mínima de bens ou serviços para comparação e controle**

    1. Cada Ordem de Serviço/Fornecimento ou Nota de Empenho conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste TR.

6. **Mecanismos formais de comunicação**

    1. São definidos como mecanismos formais de Comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

        1. Ordem de Fornecimento de Bens;

2. Ata de Reunião;
3. Ofício;
4. Sistema de abertura de chamados;
5. E-mails e Cartas;

7. **Formas de Pagamento**

1. Os critérios de medição e pagamento serão tratados em tópico específico deste Termo de Referência.

8. **Manutenção de Sigilo e Normas de Segurança**

1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução do Contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos.

2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal da CONTRATADA, e Termo de Ciência, a ser assinado por todos os empregados da CONTRATADA diretamente envolvidos na contratação, encontram-se nos ANEXOS I e II.

3. **Lei Geral de Proteção De Dados :** Em observância ao disposto na Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais:

1. É vedada às partes a utilização de todo e qualquer dado pessoal, repassado em decorrência da execução contratual, para finalidade distinta da contida no objeto da contratação, sob pena de responsabilização administrativa, civil e criminal;

2. Para fins de execução do objeto contratado e de cumprimento de obrigação legal ou regulatória, a CONTRATANTE poderá proceder ao tratamento dos dados pessoais dos representantes legais da CONTRATADA , inclusive para publicação nos portais de Transparência da CONTRATANTE;

3. Selecionada a empresa a ser CONTRATADA , para fins de assinatura do instrumento contratual, o representante legal da empresa e titular dos dados pessoais será cientificado pessoalmente do tratamento de seus dados a ser realizado pela CONTRATANTE, na forma da Declaração de Concordância e Veracidade, conforme modelo constante no Anexo V deste Termo de Referência.

7. MODELO DE GESTÃO DO CONTRATO

1. O Contrato deverá ser executado fielmente pelas partes, de acordo com as cláusulas avençadas e as normas da Lei nº 14.133, de 2021, e cada parte responderá pelas consequências de sua inexecução total ou parcial.

2. Em caso de impedimento, ordem de paralisação ou suspensão do Contrato, o cronograma de execução será prorrogado automaticamente pelo tempo correspondente, anotadas tais circunstâncias mediante simples apostila.

3. As comunicações entre o órgão ou entidade e a CONTRATADA devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

    1. **Reunião Inicial**

        1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução do Contrato.

        2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em até 5 (cinco) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da CONTRATANTE.

        3. A pauta desta reunião observará, pelo menos:

            1. Presença do representante legal da CONTRATADA , que apresentará o seu preposto;

            2. Entrega, por parte da CONTRATADA , do Termo de Compromisso e dos Termos de Ciência;

            3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do Contrato;

            4. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do Contrato e atuar como interlocutor principal junto à CONTRATANTE, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

            5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

    2. **Fiscalização**

        1. A execução do Contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do Contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

    3. **Fiscalização Técnica**

        1. O fiscal técnico do Contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do

Contrato, para que sejam cumpridas todas as condições estabelecidas no Contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

1. O fiscal técnico do Contrato anotará no histórico de gerenciamento do Contrato todas as ocorrências relacionadas à execução do Contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º , e Decreto nº 11.246, de 2022, art. 22, II);

2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do Contrato emitirá notificações para a correção da execução do Contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

3. O fiscal técnico do Contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV).

4. No caso de ocorrências que possam inviabilizar a execução do Contrato nas datas aprazadas, o fiscal técnico do Contrato comunicará o fato imediatamente ao gestor do Contrato. (Decreto nº 11.246, de 2022, art. 22, V).

5. O fiscal técnico do Contrato comunicará ao gestor do Contrato, em tempo hábil, o término do Contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

4. **Fiscalização Administrativa**

1. O fiscal administrativo do Contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022 , verificará a manutenção das condições de habilitação da CONTRATADA, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

    1. Caso ocorram descumprimento das obrigações contratuais, o fiscal administrativo do Contrato atuará tempestivamente na solução do problema, reportando ao gestor do Contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

2. Além do disposto acima, a fiscalização contratual obedecerá às rotinas previstas na Resolução TRE-PI nº 146/2008.

5. **Gestor do Contrato**

1. O gestor do Contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do Contrato contendo todos os registros formais da execução no histórico de gerenciamento do Contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das

prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do Contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV).

2. O gestor do Contrato acompanhará a manutenção das condições de habilitação da CONTRATADA, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III).

3. O gestor do Contrato acompanhará os registros realizados pelos fiscais do Contrato, de todas as ocorrências relacionadas à execução do Contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II).

4. O gestor do Contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pela CONTRATADA, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII).

5. O gestor do Contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X).

6. O fiscal técnico do Contrato comunicará ao gestor do Contrato, em tempo hábil, o término do Contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. (Decreto nº 11.246, de 2022, art. 22, VII).

7. O gestor do Contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI).

6. **Critérios de Aceitação**

1. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:

    1. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não recondicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).

    2. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda,

com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.

3. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.

4. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

5. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.

6. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.

7. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização da CONTRATANTE, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.

8. A CONTRATANTE poderá optar por avaliar a qualidade de todos os equipamentos fornecidos ou uma amostra dos equipamentos, atentando para a inclusão nos autos do processo administrativo de todos os documentos que evidenciem a realização dos testes de aceitação em cada equipamento selecionado, para posterior rastreabilidade.

9. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se ao CONTRATANTE o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no Contrato. Quando for o caso, a empresa será convocada a refazer todos os serviços rejeitados, sem custo adicional.

7. **Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento**

    1. Nos casos de inadimplemento na execução do objeto, as ocorrências serão

registradas pela CONTRATANTE, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do Contrato, salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 12 (doze) horas úteis.	Multa de 0,001% (zero virgula zero zero um porcento) sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela CONTRATANTE, até o limite de 3 (três) dias úteis. Após o limite de 3 (três) dias úteis, aplicar-se-á multa de 1% (um porcento) do valor total do Contrato. Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 1% (um porcento) do valor total do Contrato. Após o limite de 3 incidências, aplicar-se-á multa de 5% (cinco porcento) do valor total do Contrato.

2	Não entregar os bens ou prestar os serviços nos prazos previstos neste TR	Multa de 0,001% (zero virgula zero zero um porcento) sobre o valor total do Contrato por dia útil de atraso, até o limite de 3 dias úteis. Após o limite de 3 dias úteis, aplicar-se-á multa de 1% (um porcento) do valor total do Contrato. Advertência. Configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 1% (um porcento) do valor total do Contrato. Após o limite de 3 incidências, aplicar-se-á multa de 10% (dez porcento) do valor total do Contrato
3	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 1% (um porcento) do valor total do Contrato.

2. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que a CONTRATADA:

    1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

    2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8. **CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO**

1. **Recebimento do Objeto**

1. Os serviços e produtos serão recebidos provisoriamente no prazo de 5 (cinco) dias úteis da data de entrada da respectiva nota fiscal/fatura, pela unidade demandante, para efeito de posterior verificação de sua conformidade com as especificações e quantidades constantes neste Termo de Referência e na proposta/Nota fiscal.

2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de 15 (quinze) dias, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

3. O recebimento definitivo ocorrerá no prazo de 10 (dez) dias úteis, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.

4. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.

5. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento.

6. O prazo para a solução, pela CONTRATADA, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.

7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do Contrato.

2. **Liquidação**

1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022.

    1. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021.

2. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

1. o prazo de validade;
2. a data da emissão;
3. os dados do Contrato e do órgão CONTRATANTE;
4. o período respectivo de execução do Contrato;
5. o valor a pagar; e
6. eventual destaque do valor de retenções tributárias cabíveis.

3. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que a CONTRATADA providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao CONTRATANTE;

4. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta on-line ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021.

5. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).

6. Constatando-se, junto ao SICAF, a situação de irregularidade da CONTRATADA, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério da CONTRATANTE.

7. Não havendo regularização ou sendo a defesa considerada improcedente, a CONTRATANTE deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da CONTRATADA, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos.

8. Persistindo a irregularidade, a CONTRATANTE deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao CONTRATADO a ampla defesa.

9. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do Contrato, caso a CONTRATADA não regularize sua situação junto ao SICAF.

3. **Prazo de pagamento**

1. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022.

2. No caso de atraso pela CONTRATANTE, os valores devidos ao CONTRATADO serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice de 0,5% (meio por cento) ao mês, ou 6% (seis por cento) ao ano, a título de correção monetária.

4. **Forma de pagamento**

    1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela CONTRATADA.

    2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

    3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

    4. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

    5. A CONTRATADA regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

5. **Antecipação de pagamento**

    1. A presente contratação não permite a antecipação de pagamento.

6. **Cessão de crédito**

    1. Não será admitida, na presente contratação, a cessão fiduciária de direitos creditícios com instituição financeira.

9. **FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO**

1. **Forma de seleção e critério de julgamento da proposta**

    1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo menor preço.

    2. Os valores dos lances deverão observar um intervalo mínimo de 5% (cinco por cento) para cada item deste Pregão (artigo 57 da Lei 14.133/2021).

    3. Será adotado para o envio de lances o modo de disputa “aberto”, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações (artigo 18, VIII da Lei 14.133/2021).

2. **Da Aplicação da Margem de Preferência**

    1. Não será aplicada margem de preferência na presente contratação.

3. **Exigências de habilitação**

1. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

4. **Habilitação jurídica**

    1. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

    2. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

    3. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

    4. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI:** inscrição do ato constitutivo, estatuto ou Contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

    5. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020 .

    6. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

    7. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz

    8. **Sociedade** cooperativa**:** ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971 .

    9. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

5. **Habilitação fiscal, social e trabalhista**

    1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

    2. Prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02 de outubro de 2014, do Secretário da Receita

Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

4. Prova de inexistência de débitos inadimplidos perante a Justiça do Trabalho, mediante a apresentação de certidão negativa ou positiva com efeito de negativa, nos termos do Título VII-A da Consolidação das Leis do Trabalho, aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943;

5. Prova de inscrição no cadastro de contribuintes [Estadual/Distrital] ou [Municipal/Distrital] relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

6. Prova de regularidade com a Fazenda [Estadual/Distrital] ou [Municipal/Distrital] do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

7. Caso o fornecedor seja considerado isento dos tributos [Estadual/Distrital] ou [Municipal/Distrital] relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

6. **Qualificação Econômico-Financeira**

    1. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;

    2. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);

    3. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).

7. **Qualificação Técnica**

    1. Comprovação de aptidão para o fornecimento de bens similares de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso.

        1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a Contratos executados com as seguintes características mínimas:

            1. Apresentação de pelo menos 1 (um) Atestado de Capacidade Técnica, emitido por empresa de direito público ou privado, devidamente registrados nas entidades profissionais competentes,

comprovando aptidão para desempenho de atividade de fornecimento de componentes de software, treinamento, instalação, configuração e assistência técnica, compatíveis com o descrito neste Termo de Referência.

2. Todos os atestados apresentados na documentação de habilitação deverão conter, obrigatoriamente, a especificação dos serviços executados, o nome e cargo do declarante e poderão ser verificados através da diligência realizada pela CONTRATANTE.

3. Não serão aceitos protocolos de entrega ou solicitação de documento em substituição aos documentos aqui requeridos.

4. Os documentos exigidos poderão ser apresentados em original, por qualquer processo de cópia autenticada por cartório competente ou por servidor da administração, ou mediante publicação em órgão de imprensa oficial.

2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.

3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.

4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do Contrato que deu suporte à contratação, endereço atual da CONTRATANTE e local em que foi executado o objeto CONTRATADO, dentre outros documentos.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

1. O custo estimado total da contratação é de **R$ 1.292.066,93 (um milhão, duzentos e noventa e dois mil sessenta e seis reais e noventa e três centavos)**, conforme custos unitários apostos na tabela abaixo.

ID	BEM / SERVIÇO	VALOR ESTIMADO
1	Licença de Solução de Secure Web Gateway para 1.500 usuários	R$ 1.118.201,23
2	Instalação e Suporte por 36 meses	R$ 131.699,04
3	Treinamento	R$ 42.166,66
		R$ 1.292.066,93

11. ADEQUAÇÃO ORÇAMENTÁRIA

1. As despesas decorrentes da presente contratação correrão na forma especificada na

classificação da despesa a ser feita pela Coordenadoria de Orçamento e Finanças e aprovada pela Presidência deste Tribunal.

2. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

1. **Cronograma Físico Financeiro**

Evento	**Prazo estimado**	**Valor**
Fornecimento de Solução de Secure Web Gateway	Até 90 (noventa) dias após a emissão da Ordem de Fornecimento de Bens ou Nota de Empenho.	R$ 1.118.201,23
Instalação e Suporte Técnico por 36 meses	Até 30 (trinta) dias consecutivos a partir do recebimento do objeto.	R$ 131.699,04
Treinamento	Até 10 (dez) dias após a emissão nota fiscal/fatura do serviço.	R$ 42.166,66

12. **ANEXOS**

1. **Anexo I - Termo de Compromisso e Manutenção de Sigilo**
2. **Anexo II - Termo de Ciência**
3. **Anexo III - Estudos Técnicos Preliminares (0001812006)**
4. **Anexo IV - Declaração de não ocorrência do registro de oportunidade**
5. **Anexo V - Declaração de Concordância e Veracidade.**

Documento datado e assinado eletronicamente.

_____ Integrante Requisitante **Rosemberg Maia Gomes** Cordenador de Desenvolvimento e Infraestrutura Matrícula: 183	_____ Integrante Técnico **Aciel Sousa Mendes** Técnico Judiciário Matrícula: 654	_____ Integrante Administrativo **Gleidson Cavalcanti de Lima** Técnico Judiciário Matrícula: 635

Autoridade Máxima da Área de TIC
_____ **Anderson Cavalcanti de Lima** Secretário de Tecnologia da Informação Matrícula: 571

ANEXO I - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO (TCMS)

A UNIÃO FEDERAL, por intermédio do TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ, inscrito no CNPJ/MF sob o n° 05.957.363/0001-33, sediado na Praça Des. Edgar Nogueira, s/n, Teresina (PI), CONTRATANTE, e, de outro lado, a empresa _____ _____ , sediada em _____ , CNPJ n.° _____, doravante denominada CONTRATADA ;

CONSIDERANDO que, em razão do CONTRATO N. º XX/20XX, doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas da CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA , no que diz respeito ao trato de informações sensíveis e sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18 de novembro de 2011, Lei nº 13.709, de 14 de agosto de 2018, e os Decretos 7.724, de 16 de maio de 2012, e 7.845, de 14 de novembro de 2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

Informação: é o conjunto de dados organizados de acordo com procedimentos executados por meios eletrônicos ou não, que possibilitam a realização de atividades específicas e/ou tomada de decisão.

Informação Pública ou Ostensiva: são aquelas cujo acesso é irrestrito, obtida por divulgação pública ou por meio de canais autorizados pela CONTRATANTE.

Informações Sensíveis: são todos os conhecimentos estratégicos que, em função de seu potencial no aproveitamento de oportunidades ou desenvolvimento nos ramos econômicos, político, científico, tecnológico, militar e social, possam beneficiar a Sociedade e o Estado brasileiros.

Informações Sigilosas: são aquelas cujo conhecimento irrestrito ou divulgações possam acarretar qualquer risco à segurança da sociedade e do Estado, bem como aquelas necessárias ao resguardo da inviolabilidade da intimidade, da vida privada, da honra e da imagem das pessoas.

Cláusula Terceira – DAS INFORMAÇÕES SIGILOSAS

Serão consideradas como informação sigilosa, toda e qualquer informação escrita ou oral, revelada a outra parte, contendo ou não a expressão confidencial e/ou reservada.

O TERMO informação abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes.

Parágrafo Primeiro – Comprometem-se, as partes, a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas informações, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Segundo – As partes deverão cuidar para que as informações sigilosas fiquem restritas ao conhecimento das pessoas que estejam diretamente envolvidas nas atividades relacionadas à execução do objeto do CONTRATO PRINCIPAL.

Parágrafo Terceiro – As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – Sejam comprovadamente de domínio público no momento da revelação;

II – Tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – Sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quarta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem e se obrigam a utilizar a informação sigilosa revelada pela outra parte exclusivamente para os propósitos da execução do CONTRATO PRINCIPAL, em conformidade com o disposto neste TERMO.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência ao CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à

proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as informações deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA , direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA , na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das informações, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das Informações Proprietárias por seus agentes, representantes ou por terceiros;

III – Comunicar ao CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das informações, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA , terão acesso às informações sigilosas.

Cláusula Quinta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sexta – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das informações, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES.

Neste caso, a CONTRATADA , estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular

processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Arts. 155 a 163 da Lei nº. 14.133, de 2021.

Cláusula Sétima – DISPOSIÇÕES GERAIS

Este TERMO é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações deles decorrentes, ou se constatando casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

I – a CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA ;

II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL;

III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;

IV – Todas as condições, termos e obrigações ora constituídos serão regidos pela legislação e regulamentações brasileiras pertinentes;

V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;

VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;

VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA , serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;

VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar Informações Sigilosas para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Oitava – DO FORO

a CONTRATANTE elege o foro de Teresina, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes na forma eletrônica, nos termos da Lei n. 11.419/2006 e da Instrução Normativa CNJ n. 67/2015.

Pela CONTRATANTE

_____

Pela CONTRATADA

_____

ANEXO II - TERMO DE CIÊNCIA

DECLARAÇÃO DE CIÊNCIA DO TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO

PREGÃO ELETRÔNICO N° 00X/20XX

DECLARAÇÃO DE CIÊNCIA DE TCMS

O(a) Sr(a) _____[nome do(a) diretor, consultor, prestador de serviço, empregado ou preposto], CPF _____, ocupante do cargo de _____ na empresa _____, CNPJ _____, DECLARA, sob as penas da Lei, ter tomado conhecimento do TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO (TCMS), emitido por ocasião da assinatura do contrato nº _____/20__, e se compromete a seguir, naquilo que lhe couber, todas as disposições do referido Termo.

Local e data _____

Assinatura

ANEXO III - ESTUDOS TÉCNICOS PRELIMINARES (0001808506)

ANEXO IV - DECLARAÇÃO DE NÃO OCORRÊNCIA DO REGISTRO DE OPORTUNIDADE

Ao TRIBUNAL REGIONAL ELEITORAL DO PIAUÍ

A fim de garantir o princípio da competitividade no presente certame licitatório, conforme o disposto no art. 5º da Lei nº 14.133, de 2021, e no subitem 1.7 do Anexo I à **INSTRUÇÃO NORMATIVA SGD/ME Nº 94, DE 23 DE DEZEMBRO DE 2022**, que contempla as diretrizes específicas de planejamento da contratação para: 1. contratação de licenciamento de software e serviços agregados, DECLARO, para os devidos fins, que a empresa _____ **não efetuou registro de oportunidade** com o fabricante em relação ao objeto da presente contratação.

Local e data _____

CONTRATADA :

Assinatura

ANEXO V - DECLARAÇÃO DE CONCORDÂNCIA E VERACIDADE

NOME COMPLETO DO USUÁRIO:	
IDENTIDADE:	CPF:
E-MAIL DO USUÁRIO:	
LOGRADOURO:	
COMPLEMENTO:	BAIRRO:
CIDADE:	ESTADO:
TELEFONE:	CEP:

Por meio deste documento e do cadastro como Usuário Externo no SEI do TRE-PI, declaro que

aceito todos os termos e condições que disciplinam o processo eletrônico, com fundamento na legislação pertinente e especialmente no Decreto Nº 8.539, de 08/10/15, admitindo como válida a assinatura eletrônica na modalidade cadastrada (login e senha), tendo como consequência a responsabilidade pelo uso indevido das ações efetuadas, as quais serão passíveis de apuração de responsabilidade civil, penal e administrativa.

Declaro, ainda, que o endereço informado referente ao meu domicílio é verdadeiro e que são de minha exclusiva responsabilidade:

I - o sigilo da senha de acesso, não sendo oponível, alegação de uso indevido;

II - a observância de que os atos processuais em meio eletrônico se consideram realizados no dia e na hora do recebimento pelo SEI, considerando-se tempestivos os atos praticados até as 23 horas e 59 minutos e 59 segundos do último dia do prazo, considerado sempre o horário oficial de Brasília, independente do fuso horário em que se encontre o usuário externo;

III - as condições da rede de comunicação, do acesso ao provedor de internet e a configuração do computador a ser utilizado nas transmissões eletrônicas;

IV - a observância dos períodos de manutenção programada, ou qualquer outro tipo de indisponibilidade do sistema.

Por fim, nos termos da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais) e da Lei nº 12.527/2011 (Lei de Acesso à Informação), declaro ciência do tratamento dos meus dados pessoais pelo TRE-PI, inclusive para sua publicação nos portais de Transparência do Órgão.

Local e data _____

CONTRATADA :

Assinatura

Para que o acesso seja liberado e o cadastro aprovado o usuário deve acessar a página do Sistema Eletrônico de Informações – SEI do TRE-PI, por meio do seguinte canal da internet e efetuar o cadastro como usuário externo do SEI, seguindo os procedimentos indicados no documento Roteiro de cadastro de usuários externos do SEI :

https://www.tre-pi.jus.br/institucional/sistema-eletronico-de-informacoes-sei

Documento assinado eletronicamente por **Aciel Sousa Mendes**, **Técnico Judiciário**, em 06/10/2023, às 09:02, conforme art. 1º, § 2º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.tre-pi.jus.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **0001924292** e o código CRC **780BD7D3**.


2022
PRÊMIO
CNJ DE
QUALIDADE
Prata

--