ESTADO DO CEARÁ

PODER JUDICIÁRIO

SECRETARIA DE TECNOLOGIA DA INFORMAÇÃO

Termo de Referência – TR

AQSETIN2023010 - Segurança de Endpoint

PAC: TJCESETIN_2024_0011

APRESENTAÇÃO

Este Termo de Referência é sobre o objetivo de registrar uma Ata de Registro de Preço para viabilizará a contratação de empresa especializada para fornecimento de licenças de uma solução de segurança de Endpoint com funcionalidades de EDR/XDR, incluindo suporte e garantia pelo período de 60 meses. Além disso, o serviço também contempla a implantação da solução e o treinamento necessário para atender às necessidades específicas do Tribunal de Justiça do Ceará (TJCE).

1. OBJETO DA CONTRATAÇÃO

1.1. Este termo de referência tem como objeto o registro de preços para futura e eventual contratação de empresa especializada em tecnologia da informação para fornecimento de licenças de uma solução de segurança de Endpoint com funcionalidades de EDR/XDR, incluindo os serviços de instalação, configuração, implantação e treinamento da solução.

1.2. Quantitativo

Id	Objeto	Qtd.
1	Licenças de solução de segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	10.000
2	Licenças de solução de segurança de EndPoint XDR, com manutenção,	2.000

	garantia (update e upgrade), e suporte do fabricante por 60 meses.	
3	Serviços de instalação, configuração e implantação da solução.	1
4	Treinamento.	1

1.2.1. As demandas previstas com IDs 1 e 2 da Tabela mostrada acima poderão ser contratadas sob demanda de forma gradual em virtude da variação natural do número de dispositivos utilizados durante a vigência da Ata de Registro de Preços.

2. FUNDAMENTAÇÃO DA CONTRATAÇÃO

2.1. Motivação

2.1.1. A história de 150 anos do Tribunal de Justiça do Ceará (TJCE) é uma jornada marcada por avanços tecnológicos significativos, refletindo um compromisso contínuo com a modernização e a eficiência na administração da justiça. Desde a implementação do Sistema de Automação da Justiça (SAJ) em 2009, até a digitalização completa dos processos em 2019, o TJCE tem demonstrado uma forte inclinação para acompanhar e adotar as últimas tendências tecnológicas. Essas iniciativas não apenas modernizaram os processos judiciais, mas também buscaram facilitar o acesso à justiça, tornando-o mais ágil e eficiente para os cidadãos.

2.1.2. Um dos marcos mais notáveis nessa trajetória foi a introdução do Processo Judicial Eletrônico (PJe) em 2014. Concebido para otimizar o fluxo de trabalho no Judiciário, o PJe representou uma mudança fundamental na maneira como os processos eram conduzidos, reduzindo significativamente a dependência de documentos físicos e simplificando procedimentos para profissionais do Direito e partes envolvidas. Essa transição para o digital não apenas aumentou a eficiência, mas também melhorou a acessibilidade à justiça, permitindo que os usuários pudessem acompanhar seus processos de qualquer lugar.

2.1.3. Durante a pandemia de Covid-19, o TJCE enfrentou desafios sem precedentes, mas respondeu com resiliência e adaptabilidade. Implementando o regime obrigatório de teletrabalho até meados de 2021, o tribunal não apenas priorizou a segurança de seus servidores e jurisdicionados, mas também demonstrou sua capacidade de se adaptar rapidamente a circunstâncias excepcionais. Além disso, em 2021, o lançamento do "Balcão Virtual" consolidou ainda mais o compromisso do TJCE com a digitalização e a

modernização dos serviços judiciais, seguindo as diretrizes do Conselho Nacional de Justiça (CNJ).

2.1.4. No entanto, à medida que o tribunal avança em sua jornada rumo à modernização, a segurança da informação emerge como um elemento crítico na garantia da operacionalidade contínua e na proteção das informações confidenciais e sensíveis. A digitalização dos processos judiciais e a implementação de iniciativas como o teletrabalho e o Balcão Virtual introduziram novos desafios de segurança, exigindo uma abordagem proativa e holística para proteger os ativos digitais do tribunal.

2.1.5. Nesse contexto, a análise do ambiente de segurança de TI torna-se fundamental, envolvendo uma avaliação detalhada dos custos e do gerenciamento de todas as medidas de segurança relacionadas à tecnologia da informação dentro do tribunal. Isso inclui o gerenciamento de identidade e acesso, proteção da rede, segurança dos dispositivos terminais, proteção dos dados, segurança dos aplicativos, gerenciamento de vulnerabilidades e análise de segurança, além de governança, gestão de riscos e conformidade regulatória.

2.1.6. Uma solução completa de segurança de TI é essencial para proteger o TJCE contra uma ampla gama de ameaças cibernéticas. Essa solução atua como um escudo de proteção digital, integrando uma variedade de sistemas e tecnologias que trabalham em conjunto para salvaguardar contra ameaças, como malware, ransomware, phishing e outras formas de ataques. Essa defesa digital é composta por uma série de sistemas, incluindo firewalls de próxima geração, firewalls de aplicativos web, soluções de segurança de endpoint, soluções de segurança de email, gerenciamento de vulnerabilidades e soluções de backup e recuperação de dados.

2.1.7. A opção de licenciamento atual para a proteção representa o nível mais básico oferecido pelo fabricante para garantir a segurança dos endpoints corporativos. Esse nível de segurança já não é mais suficiente para atender às demandas dos dispositivos conectados à rede de dados do TJCE, isso pode trazer várias implicações na segurança e o funcionamento adequado dos sistemas do TJCE, como:

2.1.7.1. Vulnerabilidades de segurança: O nível básico de proteção pode não ser capaz de defender efetivamente os endpoints contra as ameaças cibernéticas atuais, aumentando o risco de ataques, infecções por malware e violações de dados.

2.1.7.2. Conformidade regulatória: Desconformidade das regulamentações da resolução CNJ Nº 363 de 12/01/2021, que estabelece medidas para o processo de adequação à

Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais. E da resolução CNJ Nº 396 de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

2.1.7.3. Impacto nas operações: Falhas de segurança e ataques cibernéticos podem interromper as operações normais da organização, causando tempo de inatividade, perda de produtividade e danos à reputação.

2.1.7.4. Prejuízos financeiros: Incidentes de segurança podem resultar em custos significativos, incluindo gastos com recuperação de dados, reparos de sistemas comprometidos e custos legais.

2.1.8. A quantidade atual de licenças não é mais capaz de abranger todos os dispositivos que estão atualmente em uso na rede de dados do TJCE. Assim, torna-se imprescindível adquirir licenças adicionais para garantir a cobertura atual e futura.

2.1.9. O fim do suporte aos softwares que compõem a solução atual de antivírus, em abril de 2024, pode ter diversas implicações negativas para a segurança e o funcionamento dos sistemas e dispositivos do TJCE, como:

2.1.9.1. Vulnerabilidades de segurança: Sem atualizações de segurança regulares, os softwares desatualizados podem se tornar vulneráveis a novas ameaças cibernéticas, como vírus, malware e ataques de hackers.

2.1.9.2. Falhas de desempenho: O software desatualizado pode apresentar falhas de desempenho, incluindo lentidão, travamentos e incompatibilidades com outros programas e sistemas operacionais.

2.1.9.3. Conformidade: Em muitos setores, existem requisitos regulatórios que exigem a utilização de software atualizado e suportado para proteger dados sensíveis e informações confidenciais.

2.1.9.4. Perda de suporte técnico: Sem o suporte do fabricante, o TJCE não pode obter assistência técnica para resolver problemas e realizar manutenções necessárias.

2.1.10. A evolução das soluções de antivírus e proteção de endpoint tem sido constante ao longo das últimas décadas, com novas tecnologias e técnicas sendo desenvolvidas para lidar com as ameaças cada vez mais sofisticadas que surgem no cenário de segurança cibernética.

2.1.11. As soluções de proteção de endpoint se tornaram cada vez mais integradas, com muitas soluções combinando recursos de antivírus, segurança de rede e gerenciamento de

dispositivos em uma única plataforma. A inteligência artificial e a aprendizagem de máquina também se tornaram cada vez mais comuns na detecção de ameaças e na proteção contra ataques cibernéticos sofisticados.

2.1.12. Em resumo, as soluções de antivírus e proteção de endpoint evoluíram de soluções simples de detecção de vírus para plataformas avançadas de segurança cibernética que protegem contra uma ampla variedade de ameaças em constante evolução.

2.1.13. Atualizar um antivírus para uma plataforma de segurança de endpoint avançada oferece diversas oportunidades para melhorar a postura de segurança. Aqui estão algumas das oportunidades que essa transição pode proporcionar:

2.1.13.1. Detecção Avançada de Ameaças: As plataformas de segurança de endpoint avançadas oferecem recursos de detecção avançada de ameaças, como análise comportamental, detecção de anomalias e inteligência artificial, que podem identificar e responder a ameaças de forma mais eficaz do que os antivírus tradicionais.

2.1.13.2. Prevenção de Ameaças Avançadas: Essas plataformas fornecem camadas adicionais de proteção, como prevenção de intrusões, sandboxing e aprendizado de máquina, que ajudam a impedir ataques cibernéticos avançados, como ransomware, ataques de dia zero e malware avançado.

2.1.13.3. Resposta Automatizada a Incidentes: Uma plataforma de segurança de endpoint avançada pode oferecer recursos de resposta automatizada a incidentes, que ajudam a identificar, isolar e remediar ameaças de forma rápida e eficiente, reduzindo o tempo de inatividade e o impacto nos negócios.

2.1.13.4. Visibilidade Aprimorada: Essas plataformas geralmente incluem recursos de monitoramento e relatórios avançados, que oferecem uma visão mais detalhada e em tempo real da atividade do endpoint, permitindo uma melhor compreensão das ameaças e vulnerabilidades em toda a organização.

2.1.13.5. Gerenciamento Centralizado: Uma plataforma de segurança de endpoint avançada geralmente oferece um console centralizado para gerenciamento e monitoramento de todos os endpoints da organização, facilitando a implementação de políticas de segurança consistentes e a aplicação de patches e atualizações de forma eficiente.

2.1.13.6. Conformidade Regulatória: Ao adotar uma plataforma de segurança de endpoint avançada, as organizações podem melhorar sua conformidade com regulamentações de segurança cibernética, demonstrando uma abordagem proativa para proteger os dados confidenciais dos clientes e funcionários.

2.1.14. O término do suporte aos softwares de antivírus requer uma abordagem cuidadosa e proativa para manter a segurança dos sistemas e dados da organização. É importante entender que o nível atual de proteção de endpoints pode não ser mais suficiente diante das ameaças cibernéticas em constante evolução. Portanto, é crucial tomar medidas proativas para fortalecer a segurança da organização.

2.1.15. Para isso, é necessário reconhecer a necessidade de atualizar e adquirir licenças adicionais para garantir a cobertura adequada de segurança dos dispositivos na rede de dados do TJCE. Isso ajudará a mitigar os riscos de segurança e a garantir a conformidade regulatória, além de proteger os ativos e dados da organização contra ameaças cibernéticas em constante evolução.

2.1.16. É necessário explorar opções para atualizar ou melhorar o software de segurança de endpoints, escolhendo uma solução mais robusta e adequada às necessidades atuais do TJCE.

2.1.17. A atualização de um antivírus para uma plataforma de segurança de endpoint avançada oferece uma série de oportunidades para fortalecer a solução completa de segurança de TI do TJCE.

2.1.18. Entendemos a importância da segurança da informação em todos os processos do TJCE. Isso se dá pelo fato de que a instituição lida com informações sensíveis e confidenciais, o que a torna um alvo potencial para ataques cibernéticos. E com o constante aumento das ameaças cibernéticas, é fundamental contar com uma solução que possa garantir a proteção dos endpoints utilizados pelos colaboradores do tribunal.

2.2. Resultados a serem alcançados com a contratação

2.2.1. Vinculados às necessidades de negócios.

2.2.1.1. Implementar uma estratégia abrangente de segurança de endpoint avançada: que integre prevenção, detecção e resposta, isso é essencial para garantir a proteção completa da infraestrutura de TI da TJCE. Permite uma abordagem unificada na identificação e resposta rápida às ameaças, abrangendo todos os pontos de entrada e

contando com uma interpretação baseada em comportamento para uma segurança mais eficaz.

2.2.1.2. Correlacionar eventos de segurança em toda a infraestrutura de TI: as soluções de segurança de endpoint avançada podem reduzir drasticamente o tempo necessário para detectar e responder a ameaças. Isso ajuda a minimizar o impacto das ameaças cibernéticas, protegendo proativamente a TJCE contra possíveis danos.

2.2.1.3. Simplificar a gestão de segurança: isso é outra vantagem dessas soluções integradas. Elas permitem que as equipes de segurança monitorem e gerenciem ameaças de forma mais eficiente, tudo a partir de uma única interface. Isso simplifica as operações de segurança e aumenta a capacidade de resposta da TJCE diante de incidentes de segurança.

2.2.1.4. Fornecer uma visão completa da segurança cibernética: as soluções de segurança de endpoint avançada capacitam as equipes de segurança da TJCE a tomar decisões mais informadas. Isso resulta em ações mais eficazes para lidar com ameaças e reduzir os riscos de segurança em toda a infraestrutura de TI.

2.2.1.5. Cumprir regulamentações e normas de segurança cibernética: Ao fornecer uma visão abrangente das atividades de segurança, elas facilitam a identificação e a mitigação de riscos, garantindo a conformidade com os padrões de segurança estabelecidos.

2.2.1.6. Utilizar sistemas especializados em segurança da informação para aprimorar a confidencialidade, integridade e disponibilidade dos dados que circulam na rede do TJCE.

2.2.1.6.1. Dados processuais: informações pertinentes aos processos judiciais.

2.2.1.6.2. Dados pessoais: informações de caráter pessoal dos envolvidos nos processos, abarcando nomes, endereços, números de documentos, antecedentes criminais, dados biométricos, entre outros.

2.2.1.6.3. Documentação digital: documentos eletrônicos empregados no ambiente de trabalho do TJCE.

2.2.1.6.4. Comunicações internas: correspondência eletrônica, mensagens instantâneas, chamadas de voz e videoconferências realizadas pelos colaboradores do TJCE.

2.2.1.6.5. Informações de segurança: registros de acesso, registros de eventos, detalhes de autenticação, registros de monitoramento e outras informações associadas à segurança da rede e dos sistemas do TJCE.

2.2.1.6.6. Dados dos sistemas administrativos: informações relativas à administração interna do TJCE, incluindo recursos humanos, finanças, compras, contratos, licitações e demais áreas afins.

2.2.1.7. Implementar uma solução avançada de detecção e resposta a incidentes de endpoint para aprimorar a segurança dos dispositivos e serviços utilizados pelos usuários da rede do TJCE, atendendo às seguintes necessidades de negócios:

2.2.1.7.1. Segurança da Informação: No TJCE, lidamos com uma grande quantidade de informações confidenciais, sensíveis e sigilosas. A detecção e resposta a incidentes de segurança em endpoints desempenha um papel essencial na proteção dessas informações contra ameaças cibernéticas, violações de segurança e acesso não autorizado.

2.2.1.7.2. Integridade dos Sistemas: Os sistemas do TJCE são fundamentais para o funcionamento adequado das atividades judiciais. A detecção e resposta a incidentes em endpoints contribuem para manter a integridade desses sistemas, prevenindo e mitigando incidentes que possam comprometer a disponibilidade e o desempenho dos mesmos.

2.2.1.7.3. Continuidade dos Serviços: A detecção e resposta a incidentes em enpoints desempenham um papel crucial na garantia da continuidade dos serviços do TJCE. Isso minimiza o impacto e assegura que os serviços sejam restaurados o mais rapidamente possível em caso de interrupções ou ataques cibernéticos.

2.2.1.8. Implementar políticas de segurança personalizadas para atender às necessidades específicas do TJCE.

2.2.1.9. Minimizar os riscos de vazamento de informações sensíveis e confidenciais.

2.2.1.10. Cumprir com a conformidade das normas e regulamentos aplicáveis.

2.2.1.10.1. Resolução CNJ Nº 363 de 12/01/2021, que estabelece medidas para o processo de adequação à Lei Geral de Proteção de Dados Pessoais a serem adotadas pelos tribunais.

2.2.1.10.2. Resolução CNJ Nº 396 de 07/06/2021, que institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário.

2.2.1.10.3. Resolução do Órgão Especial TJCE nº 15, de 06/07/2023 que

regulamenta a Política de Segurança da Informação no âmbito do Poder Judiciário do Estado do Ceará.

2.2.1.11. Contar com soluções de tratamento e resposta a incidentes de endpoints, com o objetivo de atender os seguintes artigos específicos da RESOLUÇÃO No 396, DE 7 DE JUNHO DE 2021 do CNJ:

2.2.1.11.1. Art. 6º, Inciso IV: permitir a manutenção e a continuidade dos serviços, ou o seu restabelecimento em menor tempo possível.

2.2.1.11.2. Art. 9º, Inciso II: elevar o nível de segurança das infraestruturas críticas.

2.2.1.11.3. Art. 11º, Inciso I: estabelecer todas as ações que possibilitem maior eficiência, ou seja, capacidade de responder de forma satisfatória a incidentes de segurança, permitindo a contínua prestação dos serviços essenciais a cada órgão.

2.2.1.11.4. Art. 11º, Inciso III: elaborar e aplicar processo de resposta e tratamento a incidentes de segurança cibernética que contenha, entre outros, procedimento de continuidade do serviço prestado e seu rápido restabelecimento, além de comunicação interna e externa.

2.2.1.11.5. Art. 11º, Inciso XI: realizar prática em gestão de incidentes e efetivar o aprimoramento contínuo do processo.

2.2.1.11.6. Art. 12º, Inciso V: possibilitar a convergência de esforços e iniciativas na apuração de incidentes e na promoção de ações de capacitação e educação em segurança cibernética.

2.2.2. Ampliação da visibilidade e fortalecimento da segurança da informação.

2.2.3. Aumento da inteligência e maturidade em segurança em TI.

2.2.4. Vinculados às necessidades tecnológicas.

2.2.4.1. Contar com soluções de segurança da informação para tratamento e resposta a incidentes em endpoints com o objetivo de atender os seguintes artigos da RESOLUÇÃO No 396, DE 7 DE JUNHO DE 2021 do CNJ:

2.2.4.1.1. Art. 11º, Inciso IV: utilizar tecnologia que possibilite a análise consolidada dos registros de auditorias coletados em diversas fontes de ativos de informação e de ações de usuários, permitindo automatizar ações de segurança e oferecer inteligência à análise de eventos de segurança.

2.2.4.1.2. Art. 11º, Inciso VI: providenciar a realização de cópias de segurança atualizadas e segregadas de forma automática em local protegido, em

formato que permita a investigação de incidentes.

2.2.4.2. Treinamento especializado para repasse de conhecimento do serviço técnico especializado.

2.2.4.3. Automatização de tarefas repetitivas e rotineiras, possibilitando que a equipe de segurança direcione seus esforços para atividades críticas, ao mesmo tempo em que fortalece a confiança dos usuários nos serviços oferecidos pelo TJCE.

2.2.4.4. Detectar e responder às ameaças cibernéticas com agilidade e eficiência, diminuindo o tempo de inatividade não programado e mitigando os efeitos das violações de segurança.

2.2.4.5. Aprimorar a investigação de incidentes de segurança da informação por meio da coleta de informações detalhadas, com o objetivo de melhorar a segurança de maneira abrangente e eficaz.

2.2.4.6. Analisar o comportamento dos endpoints e identificar atividades suspeitas, para detectar comportamentos maliciosos e prevenir possíveis ataques.

2.2.4.7. Identificar e bloquear ameaças avançadas e malware em endpoints, incluindo ransomware e outras variedade de ameaças em constante evolução.

2.2.4.8. Gerenciar patches e atualizações de segurança dos sistemas dos dispositivos utilizados pelos colaboradores do TJCE.

2.2.4.9. Gerar relatórios de segurança e conformidade para análise e gerenciamento do ambiente de TI.

2.2.4.10. Dispor de capacidade de investigar e corrigir quaisquer ameaças cibernéticas nos dispositivos mencionados que conseguirem burlar os controles de proteção existentes.

2.2.4.11. Possuir disponibilidade de recursos para reduzir a superfície de ataque, detectar, investigar e responder a incidentes de segurança da informação em computadores desktop, laptops, servidores e dispositivos móveis institucionais.

2.2.4.12. Aperfeiçoar a investigação de incidentes segurança da informação ao coletar informações detalhadas de comportamentos anormais em computadores desktop, laptops, servidores e dispositivos móveis institucionais.

2.2.4.13. Haver uma proteção adicional de segurança da informação avançada de Endpoint nos servidores.

2.2.4.14. Contribuir para o fluxo de informações de segurança e incidentes cibernéticos do TCE, fornecendo dados essenciais às equipes de resposta a

incidentes e ao Centro de Operações de Segurança (SOC), de modo a possibilitar a ação imediata na prevenção de ameaças digitais. Isso inclui:

2.2.4.14.1. Tentativas de inserção de dados fraudulentos nos sistemas, com potencial para causar danos e disseminar informações incorretas.

2.2.4.14.2. O roubo de dados privados, uma questão de grande importância para o TJCE, dada a sensibilidade dos dados sob sua responsabilidade.

2.2.4.14.3. A apropriação indevida de credenciais de acesso de servidores, o que pode resultar em sérias violações de segurança.

2.2.4.14.4. Ataques de ransomware direcionados aos servidores, representando uma ameaça significativa que pode prejudicar a integridade dos sistemas.

2.3. Referência aos Estudos Técnicos Preliminares

2.3.1. Os documentos originados dos Estudos Técnicos Preliminares deste processo de contratação foram devidamente anexados aos registros correspondentes no Processo Administrativo relacionado à demanda detalhada neste Termo de Referência (TR).

2.4. Alinhamento estratégico

ID	Objetivo Estratégico Institucional	ID	Objetivos de Contribuição da SETIN
01	Fortalecer a inteligência de dados e a segurança da informação	01	Proporcionar segurança, disponibilidade e confiabilidade às informações dos sistemas, plataformas e ferramentas institucionais

ID	Iniciativa Elencada no PDTIC 2023
N23121	Aquisição de antivírus (endpoint)

2.5. Critérios Ambientais

2.5.1. A Contratada deverá providenciar o recolhimento e o adequado descarte de produto(s) e material(is) inservível(is) originário(s) da contratação, recolhendo-os aos pontos de coleta ou centrais de armazenamentos mantidos pelo respectivo fabricante ou importador, para fins de sua destinação final ambientalmente adequada, nos termos da Instrução Normativa IBAMA n° 01, de 18/03/2010, da Lei n° 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA n° 416, de 30/09/2009,

e legislação correlata.

2.5.2. A Contratada deverá contribuir para a promoção do desenvolvimento nacional sustentável no cumprimento de diretrizes e critérios de sustentabilidade ambiental, de acordo com o art. 225 da Constituição Federal/88, e em conformidade com o art. 11º da Lei n.º 14.133/21.

2.5.3. Que os bens sejam constituídos, no todo ou em parte, por material reciclado, atóxico, biodegradável, conforme ABNT NBR – 15448-1 e 15448-2.

2.5.4. Que os bens devam ser preferencialmente, acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento.

2.5.5. Que os bens não contenham substâncias perigosas em concentração acima da recomendada na diretiva ROHS (*restriction of certain hazardous substances*), tais como mercúrio (hg), chumbo (pb), cromo hexavalente (cr(vi)), cádmio (cd), bifenil-polibromados (pbbs), éteres difenil-polibromados (pbdes).

2.5.6. Os serviços prestados e os bens fornecidos pela Contratada deverão pautar-se sempre no uso racional de recursos e equipamentos, de forma a evitar e prevenir o desperdício de insumos e materiais consumidos bem como a geração excessiva de resíduos, a fim de atender às diretrizes de responsabilidade ambiental adotadas pela TJCE.

2.6. Pesquisa de preços de mercado.

2.6.1. A pesquisa de mercado está presente no documento acostado aos autos do processo.

2.7. Natureza do Objeto

2.7.1. A natureza do objeto a ser licitado é comum de acordo com o inciso XIII do art. 6°, da Lei 14.133, de 1º de abril de 2021, que considera bens e serviços comuns, aqueles cujos padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais.

2.8. Natureza do Serviço

2.8.1. Os serviços especializados a serem contratados, identificados no item 1.2 como 3 (Serviços de instalação, configuração e implantação da solução) e 4 (Treinamento), devem ser serviços não contínuos ou contratados por escopo: aqueles que impõem ao contratado o dever de realizar a prestação de um serviço específico em período predeterminado, podendo ser prorrogado, desde que justificadamente, pelo prazo

necessário à conclusão do objeto.

2.9. Justificativa para Aplicação do Direito de Preferência (Lei complementar nº 123/06 e Lei nº 8.248/91)

2.9.1. Nos termos do art. 48, III da Lei Complementar n. 123, de 2006 (atualizada pela LC n. 147/2014), a Administração deverá estabelecer, em certames para aquisição de bens de natureza divisível, cota de até 25% (vinte e cinco por cento) do objeto para a contratação de microempresas e empresas de pequeno porte. Por essa razão, parcela de até 25% (vinte e cinco por cento) dos quantitativos divisíveis deverão ser destinados exclusivamente a ME/EPP/COOP beneficiadas pela LC n. 123/2006. Essas "cotas reservadas" deverão ser definidas em função de cada item separadamente ou, nas licitações por preço global, em função do valor estimado para o grupo ou o lote da licitação que deve ser considerado como um único item (art. 9º, inciso I do Decreto n. 8.538, de 2015).

2.9.2. In casu, a licitação que se pretende deverá ocorrer pelo menor preço global. Contudo, todos os itens se trata de serviços interdependentes em sua totalidade, sendo 4 (quadro) itens, não havendo, desta forma, como fazê-lo divisível sem desnaturá-lo.

2.9.3. Para tanto, o Art 39 da Lei Nº 15.306 , de 08 de janeiro de 2013 do Estado do Ceará excepciona algumas hipóteses, quais sejam: *II - não houver um mínimo de 3 (três) fornecedores competitivos enquadrados como microempresas ou empresas de pequeno porte sediados no Estado e capazes de cumprir as exigências estabelecidas no instrumento convocatório, exceto quando se tratar de incentivo à inovação tecnológica ou de serviços de informática; III - o tratamento diferenciado e simplificado para as microempresas e empresas de pequeno porte não for vantajoso para a Administração Pública Estadual ou representar prejuízo ao conjunto ou complexo do objeto a ser contratado e à economia de escala;*.

2.9.4. No caso aqui exposto, com toda a contextualização elaborada até então, fica evidente que o inciso III se amolda à situação ora posta, já vez que por se tratar de solução e serviços não divisíveis, não caberia particionar a entrega dos itens do lote entre fornecedores distintos.

2.9.5. Considera-se "não vantajosa a contratação" quando: *§ 1º Para fins do disposto no inciso III, considera-se não vantajoso para a Administração quando o tratamento diferenciado e simplificado não for capaz de alcançar os objetivos previstos no art. 30 desta Lei, justificadamente, ou resultar em preço superior ao valor estabelecido como referência*. (Lei Nº 15.306, de 08 de janeiro de 2013 do Estado do Ceará, Art.

39).

2.9.6. Diante do explanado, conclui-se que não há óbice quanto à aplicação da Lei Complementar 123/2006. Entretanto não é possível a divisão ou fragmentação dos itens em partes e nem aplicação do benefício da exclusividade para que ocorra a participação para ME/EPP, ante da impossibilidade da divisão técnica dos itens, conforme explanação apresentada neste Termo de Referência.

2.10. Da Subcontratação, Cisão ou Incorporação

2.10.1. Não será permitida a subcontratação total ou parcial do objeto.

2.10.2. Será admissível a fusão, cisão ou incorporação da Contratada em outra pessoa jurídica, sob a condição de que a nova pessoa jurídica cumpra todas as exigências de habilitação que eram requeridas na licitação original, além de preservar as demais cláusulas e condições do contrato em vigor, não prejudicar a execução do objeto contratual e obter a autorização expressa da Administração para a continuidade do contrato.

2.11. Justificativa para utilização do sistema de registro de preços

2.11.1. A utilização do Sistema de Registro de Preços (SRP) se justifica pela sua eficácia em proporcionar economia, agilidade e transparência nas aquisições públicas, conforme estabelecido na Lei de Licitações e Contratos Administrativos (Lei nº 14.133, de 1º de abril de 2021). O SRP permite que órgãos públicos como o Tribunal de Justiça do Ceará (TJCE) registrem preços para a aquisição de bens e serviços comuns, como licenças de software de segurança de Endpoint, conforme necessário ao longo de um período pré-determinado.

2.11.2. Ao adotar o SRP, o TJCE tem a oportunidade de obter preços mais vantajosos por meio de economias de escala, uma vez que as licenças serão registadas em quantidades maiores, proporcionando ganhos de eficiência e redução de custos. Além disso, o SRP permite flexibilidade para a aquisição conforme a demanda surgir ao longo do período de vigência da ata de registro de preços, respeitando os princípios da economicidade e da eficiência na administração pública.

2.11.3. A utilização do Sistema de Registro de Preços se mostra como uma alternativa eficaz e alinhada com os princípios da administração pública para a aquisição de licenças de software de segurança de Endpoint.

3. DESCRIÇÃO DA SOLUÇÃO

3.1. Aquisição de uma solução de segurança de endpoint, para prever, prevenir, detectar e responder a ciberataques de maneira holística, otimizada, integrada e simplificada, no âmbito do Tribunal de Justiça do Estado do Ceará (TJCE).

3.2. Deve ser fornecido o software de antivírus com EDR/XDR de acordo com o quantitativo previsto, com download do site do fabricante com devido licenciamento.

3.3. Deve ser validada a ferramenta de gerenciamento da plataforma, comprovando perante o fabricante que se trata de uma ferramenta devidamente licenciada.

3.4. Especificação técnica mínima Solução de Segurança de EndPoint

3.4.1. **Servidor de Administração e Console Gerenciamento**

3.4.1.1. **Características:**

3.4.1.1.1. A console deve ser acessada via WEB (HTTPS);

3.4.1.1.2. A console deve suportar arquitetura cloud-based;

3.4.1.1.3. Console deve ser baseada no modelo cliente/servidor;

3.4.1.1.4. A console deve suportar autenticação de dois fatores;

3.4.1.1.5. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;

3.4.1.1.6. Deve permitir incluir usuários do AD para logarem na console de administração

3.4.1.1.7. Console deve ser totalmente integrada com suas funções e módulos, caso haja a necessidade no futuro de adicionar novas tecnologias tais como, criptografia, gerenciamento de vulnerabilidades, detecção e resposta de endpoint, avaliação de vulnerabilidades, gerenciamento de dispositivos moveis;

3.4.1.1.8. As licenças deverão ser perpétuas, ou seja, expirado a validade da mesma o produto deverá permanecer funcional para a proteção contra códigos maliciosos utilizando as definições até o momento da expiração da licença;

3.4.1.1.9. Deverá ser possível buscar novos produtos e soluções a partir da console;

3.4.1.1.10. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;

3.4.1.1.11. Capacidade de instalar remotamente a solução de antivírus nas estações e servidores Windows, através de compartilhamento administrativo, através da console de gerenciamento e GPO de AD.

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

3.4.1.1.13. Deve armazenar histórico das alterações feitas em políticas;

3.4.1.1.14. Deve permitir voltar para uma configuração antiga da política de acordo com o histórico de alterações efetuadas pelo administrador apenas selecionando a data em que a política foi alterada;

3.4.1.1.15. Deve ter a capacidade de comparar a política atual com a anterior, informando quais configurações foram alteradas;

3.4.1.1.16. A solução de gerência deve permitir, através da console de gerenciamento, visualizar o número total de licenças gerenciadas;

3.4.1.1.17. Através da solução de gerência, deve ser possível verificar qual licença está aplicada para determinado computador;

3.4.1.1.18. A solução de gerência centralizada deve permitir gerar relatórios, visualizar eventos, gerenciar políticas e criar painéis de controle;

3.4.1.1.19. Deverá ter a capacidade de criar regras para limitar o tráfego de comunicação cliente/servidor por subrede com os seguintes parâmetros: KB/s e horário;

3.4.1.1.20. Capacidade de gerenciar estações de trabalho e servidores de arquivos (tanto Windows como Linux e Mac) protegidos pela solução antivírus;

3.4.1.1.21. Capacidade de gerenciar smartphones e tablets (Android e iOS) protegidos pela solução de segurança;

3.4.1.1.22. Capacidade de instalar atualizações em computadores de teste antes de instalar nos demais computadores da rede;

3.4.1.1.23. Capacidade de gerar pacotes customizados (auto executáveis) contendo a licença e configurações do produto;

3.4.1.1.24. Capacidade de atualizar os pacotes de instalação com as últimas vacinas;

3.4.1.1.25. Capacidade de fazer distribuição remota de qualquer software, ou seja, deve ser capaz de remotamente enviar qualquer software pela estrutura de gerenciamento de antivírus para que seja instalado nas máquinas clientes;

3.4.1.1.26. A comunicação entre o cliente e o servidor de administração deve ser criptografada;

3.4.1.1.27. Capacidade de desinstalar remotamente qualquer software instalado nas máquinas clientes;

3.4.1.1.28. Deve permitir a realocação de máquinas novas na rede para um determinado grupo sem ter um agente ou endpoint instalado utilizando os seguintes parâmetros:

3.4.1.1.29. Nome do computador;

3.4.1.1.30. Nome do domínio;

3.4.1.1.31. Range de IP;

3.4.1.1.32. Sistema Operacional;

3.4.1.1.33. Máquina virtual.

3.4.1.1.34. Capacidade de importar a estrutura do Active Directory para descobrimento de máquinas;

3.4.1.1.35. Deve ter a capacidade de descobrir novos dispositivos na rede, utilizando as seguintes técnicas:

3.4.1.1.36. Pesquisa de rede (Windows pooling);

3.4.1.1.37. Pesquisa ativa do AD (AD pooling);

3.4.1.1.38. Pesquisa de IP (IP pooling);

3.4.1.1.39. Pesquisa de rede (Zeroconf pooling);

3.4.1.1.40. Deve permitir, por meio da console de gerenciamento, extrair um artefato em área de backup de um cliente sem a necessidade de um servidor ou console de quarentena adicional;

3.4.1.1.41. Capacidade de monitorar diferentes subnets de rede a fim de encontrar máquinas novas para serem adicionadas à proteção;

3.4.1.1.42. Capacidade de monitorar grupos de trabalhos já existentes e quaisquer grupos de trabalho que forem criados na rede, a fim de encontrar máquinas novas para serem adicionadas a proteção;

3.4.1.1.43. Capacidade de, assim que detectar máquinas novas no Active Directory, subnets ou grupos de trabalho, automaticamente importar a máquina para a estrutura de proteção da console e verificar se possui o antivírus instalado. Caso não possuir, deve instalar o antivírus automaticamente;

3.4.1.1.44. Capacidade de agrupamento de máquina por características comuns entre as mesmas, por exemplo: agrupar todas as máquinas que não tenham o antivírus instalado, agrupar todas as máquinas que não receberam atualização nos últimos 2 dias, etc;

3.4.1.1.45. Capacidade de definir políticas de configurações diferentes por grupos de estações, permitindo que sejam criados subgrupos e com função de herança de políticas entre grupos e subgrupos;

3.4.1.1.46. Deve fornecer as seguintes informações dos computadores:

3.4.1.1.47. Se o antivírus está instalado;

3.4.1.1.48. Se o antivírus está iniciado;

3.4.1.1.49. Se o antivírus está atualizado;

3.4.1.1.50. Minutos/horas desde a última conexão da máquina com o servidor administrativo;

3.4.1.1.51. Minutos/horas desde a última atualização de vacinas;

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

3.4.1.1.53. Versão do antivírus instalado na máquina;

3.4.1.1.54. Se é necessário reiniciar o computador para aplicar mudanças;

3.4.1.1.55. Quantidade de vírus encontrados (contador) na máquina;

3.4.1.1.56. Nome do computador;

3.4.1.1.57. Domínio ou grupo de trabalho do computador;

3.4.1.1.58. Data e horário da última atualização de vacinas;

3.4.1.1.59. Sistema operacional com Service Pack;

3.4.1.1.60. Quantidade de processadores;

3.4.1.1.61. Quantidade de memória RAM;

3.4.1.1.62. Sessões de usuários, com informações de contato (caso disponíveis no Active Directory);

3.4.1.1.63. Endereço IP;

3.4.1.1.64. Aplicativos instalados, inclusive aplicativos de terceiros, com histórico de instalação, contendo data e hora que o software foi instalado ou removido;

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

3.4.1.1.66. Vulnerabilidades de aplicativos instalados na máquina;

3.4.1.1.67. Deve permitir bloquear as configurações do antivírus instalado nas estações e servidores de maneira que o usuário não consiga alterá-las;

3.4.1.1.68. Capacidade de reconectar máquinas clientes ao servidor administrativo mais próximo, baseado em regras de conexão como:

3.4.1.1.69. Alteração de Gateway Padrão;

3.4.1.1.70. Alteração de subrede;

3.4.1.1.71. Alteração de domínio;

3.4.1.1.72. Alteração de servidor DHCP;

3.4.1.1.73. Alteração de servidor DNS;

3.4.1.1.74. Alteração de servidor WINS;

3.4.1.1.75. Resolução de Nome;

3.4.1.1.76. Disponibilidade de endereço de conexão SSL;

3.4.1.1.77. Capacidade de configurar políticas móveis para que quando um

computador cliente estiver fora da estrutura de proteção possa atualizar-se via internet;

3.4.1.1.78. Capacidade de instalar outros servidores administrativos para balancear a carga e otimizar tráfego de link entre sites diferentes;

3.4.1.1.79. Capacidade de relacionar servidores em estrutura de hierarquia para obter relatórios sobre toda a estrutura de antivírus;

3.4.1.1.80. A console de gerenciamento deve suportar funções de controle de acesso com base na função (RBAC) para a hierarquia de servidores;

3.4.1.1.81. Capacidade de herança de tarefas e políticas na estrutura hierárquica de servidores administrativos;

3.4.1.1.82. Capacidade de herança de configuração de tarefas, políticas e relatórios na estrutura de hierarquia de servidores on-premisse com servidor em cloud.

3.4.1.1.83. Capacidade de eleger qualquer computador cliente como repositório de vacinas e de pacotes de instalação, sem que seja necessária a instalação de um servidor administrativo completo, onde outras máquinas clientes irão atualizar-se e receber pacotes de instalação, a fim de otimizar tráfego da rede;

3.4.1.1.84. Capacidade de fazer deste repositório de vacinas um gateway para conexão com o servidor de administração, para que outras máquinas que não consigam conectar-se diretamente ao servidor possam usar este gateway para receber e enviar informações ao servidor administrativo;

3.4.1.1.85. Capacidade de exportar relatórios para os seguintes tipos de arquivos: PDF, HTML e XML;

3.4.1.1.86. Capacidade de monitoramento do sistema através de um SNMP client;

3.4.1.1.87. Capacidade enviar eventos através de protocolo de syslog;

3.4.1.1.88. Capacidade exportar eventos para sistemas de SIEM no formato LEEF e CEF.

3.4.1.1.89. Deve ser capas de enviar os eventos para sistemas de SIEM em canal encriptado.

3.4.1.1.90. Dever ter a capacidade de exportar eventos para sistemas de SIEM, compatível com Qradar, ArcSight e Splunk.

3.4.1.1.91. Capacidade de enviar e-mails para contas específicas em caso de algum evento;

3.4.1.1.92. Listar em um único local, todos os computadores não gerenciados na rede;

3.4.1.1.93. Deve encontrar computadores na rede através de no mínimo três formas:

Domínio, Active Directory e subredes;

3.4.1.1.94. Capacidade de baixar novas versões do antivírus direto pela console de gerenciamento, sem a necessidade de importá-los manualmente

3.4.1.1.95. Capacidade de ligar máquinas via Wake on Lan para realização de tarefas (varredura, atualização, instalação, etc), inclusive de máquinas que estejam em subnets diferentes do servidor;

3.4.1.1.96. Capacidade de habilitar automaticamente uma política caso ocorra uma epidemia na rede (baseado em quantidade de vírus encontrados em determinado intervalo de tempo);

3.4.1.1.97. Deve através de opções de optimizações fazer com que o computador gerenciado conceda recursos à outras aplicações, mantendo o antivírus ativo, porém sem comprometer o desempenho do computador;

3.4.1.1.98. Deve permitir a configuração de senha no endpoint e configurar quando que será necessário a utilizá-la, (ex: Solicitar senha quando alguma tarefa de scan for criada localmente no endpoint);

3.4.1.1.99. Deve ser capaz de configurar quais eventos serão armazenados localmente, nos eventos do windows ou ainda se serão mostrados na tela para o colaborador, sejam estes eventos informativos, de alertas ou de erros;

3.4.1.1.100. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

3.4.1.1.101. Deve armazenar localmente e enviar ao servidor de gerência a ocorrência de vírus com os seguintes dados, no mínimo:

3.4.1.1.102. Nome do vírus;

3.4.1.1.103. Nome do arquivo infectado;

3.4.1.1.104. Data e hora da detecção;

3.4.1.1.105. Nome da máquina ou endereço IP;

3.4.1.1.106. Ação realizada.

3.4.1.1.107. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

3.4.1.1.108. Capacidade de listar updates nas máquinas com o respectivo link para download;

3.4.1.1.109. Deve criar um backup de todos arquivos deletados em computadores durante a desinfecção para que possam ser restaurados;

3.4.1.1.110. Deve ter uma área de backup na própria console de gerenciamento, permitindo baixar um artefato ou enviar direto para análise do fabricante;

3.4.1.1.111. Capacidade de realizar resumo de hardware de cada máquina cliente;

3.4.1.1.112. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

3.4.2. **Sistemas operacionais Windows**

3.4.2.1. **Deve ser compatível com os seguintes sistemas de estação de trabalho:**

3.4.2.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

3.4.2.1.2. Microsoft Windows 8 Professional/Enterprise;

3.4.2.1.3. Microsoft Windows 8.1 Professional / Enterprise;

3.4.2.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

3.4.2.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

3.4.2.2. **Deve ser compatível com os seguintes sistemas servidores:**

3.4.2.2.1. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

3.4.2.2.2. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

3.4.2.2.3. Windows Server 2016 Essentials / Standard / Datacenter;

3.4.2.2.4. Windows Server 2019 Essentials / Standard / Datacenter;

3.4.2.2.5. Windows Server 2022.

3.4.2.3. **Suporta as seguintes plataformas virtuais:**

3.4.2.3.1. Vmware Workstation 16.2.3;

3.4.2.3.2. Vmware ESXi 7.0 Update 3d;

3.4.2.3.3. Microsoft Hyper-V Server 2019;

3.4.2.3.4. Citrix Hypervisor 8.2

3.4.2.4. **Características:**

3.4.2.4.1. Deve prover as seguintes proteções:

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

3.4.2.4.3. Antivírus de Web (módulo para verificação de sites e downloads contra vírus);

3.4.2.4.4. O Endpoint deve possuir opção para rastreamento por linha de comando, parametrizável, com opção de limpeza;

3.4.2.4.5. Deve possui modulo dedicado contra prevenção de intrusão, Prevenção

de intrusão do host;

3.4.2.4.6. Autoproteção (contra-ataques aos serviços/processos do antivírus);

3.4.2.4.7. Controle de dispositivos externos;

3.4.2.4.8. Controle de acesso a sites por categoria, ex: Bloquear conteúdo adulto, sites de jogos, etc;

3.4.2.4.9. Controle de acesso a sites por horário;

3.4.2.4.10. Controle de acesso a sites por usuários;

3.4.2.4.11. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de vídeo e áudio;

3.4.2.4.12. Controle de execução de aplicativos;

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

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

3.4.2.4.15. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

3.4.2.4.16. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.4.2.4.17. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

3.4.2.4.18. Capacidade de adicionar aplicativos a uma lista de “aplicativos confiáveis”, onde as atividades de rede, atividades de disco e acesso ao registro do Windows não serão monitoradas;

3.4.2.4.19. Deverá possuir módulo dedicado para proteção contra port scanning;

3.4.2.4.20. Deverá possuir módulo dedicado para proteção contra network flooding;

3.4.2.4.21. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

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

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

da extensão do arquivo;

3.4.2.4.24. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;

3.4.2.4.25. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.

3.4.2.4.26. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.

3.4.2.4.27. Deverá realizar scanner de firmaware em busca de rootkits.

3.4.2.4.28. Ao detectar uma ameaça, a solução deve exibir informações:

3.4.2.4.29. Do objeto SHA256;

3.4.2.4.30. Do objeto MD5.

3.4.2.4.31. Capacidade de verificar somente arquivos novos e alterados;

3.4.2.4.32. Capacidade de verificar objetos usando heurística;

3.4.2.4.33. Capacidade de agendar uma pausa na verificação;

3.4.2.4.34. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;

3.4.2.4.35. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;

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

3.4.2.4.37. Perguntar o que fazer, ou;

3.4.2.4.38. Bloquear acesso ao objeto;

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

3.4.2.4.40. Caso positivo de desinfecção:

3.4.2.4.41. Restaurar o objeto para uso;

3.4.2.4.42. Caso negativo de desinfecção:

3.4.2.4.43. Mover para uma área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

3.4.2.4.45. Capacidade de verificar todo o tráfego web de acessos à internet nos protocolos HTTP, HTTPS e FTP, utilizando técnicas de banco de dados, serviços da nuvem do fabricante e análise de heurística bloqueado arquivos, sites de phishing e URL maliciosas;

3.4.2.4.46. Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);

3.4.2.4.47. Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Tráfego de rede por aplicativo.

3.4.2.4.48. Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;

3.4.2.4.49. Na verificação de tráfego web, caso encontrado código malicioso o programa deve:

3.4.2.4.50. Perguntar o que fazer, ou;

3.4.2.4.51. Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;

3.4.2.4.52. Permitir acesso ao objeto;

3.4.2.4.53. O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:

3.4.2.4.54. Verificação *on-the-fly*, onde os dados são verificados enquanto são recebidos em tempo-real, ou;

3.4.2.4.55. Verificação de *buffer*, onde os dados são recebidos e armazenados para posterior verificação;

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

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

3.4.2.4.58. Deve possuir módulo que analise qualquer tentativa de edição, exclusão ou gravação do registro, de forma que seja possível escolher chaves específicas para serem monitoradas e/ou bloqueadas;

3.4.2.4.59. Deve possuir módulo de bloqueio de *Phishing*, com atualizações incluídas nas vacinas, obtidas pelo *Anti-Phishing Working Group* (http://www.antiphishing.org/);

3.4.2.4.60. Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;

3.4.2.4.61. Deve possuir módulo para proteção contra *port scans, network flooding e MAC spoofing*. A base de dados de análise deve ser atualizada juntamente com as vacinas;

3.4.2.4.62. Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;

3.4.2.4.63. Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.

3.4.2.4.64. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.4.2.4.65. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

3.4.2.4.66. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.4.2.4.67. Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

3.4.2.4.68. Discos de armazenamento locais;

3.4.2.4.69. Armazenamento removível;

3.4.2.4.70. Impressoras;

3.4.2.4.71. CD/DVD;

3.4.2.4.72. Drives de disquete;

3.4.2.4.73. Modems;

3.4.2.4.74. Dispositivos de fita;

3.4.2.4.75. Dispositivos multifuncionais;

3.4.2.4.76. Leitores de smart card;

3.4.2.4.77. Wi-Fi;

3.4.2.4.78. Adaptadores de rede externos;

3.4.2.4.79. Dispositivos MP3 ou smartphones;

3.4.2.4.80. Dispositivos Bluetooth;

3.4.2.4.81. Câmeras e Scanners.

3.4.2.4.82. Capacidade de liberar acesso a um dispositivo e usuários por um período de tempo específico, sem a necessidade de desabilitar a proteção e o gerenciamento central ou de intervenção local do administrador na máquina do usuário;

3.4.2.4.83. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;

3.4.2.4.84. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;

3.4.2.4.85. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.

3.4.2.4.86. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.

3.4.2.4.87. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;

3.4.2.4.88. Capacidade de limitar a execução de aplicativos por hash MD5, nome do arquivo, versão do arquivo, nome do aplicativo, versão do aplicativo, fabricante/desenvolvedor, categoria (ex: navegadores, gerenciador de download, jogos, aplicação de acesso remoto, etc);

3.4.2.4.89. Ter a capacidade de detectar a modificação de firmware em dispositivos USB mal-intencionado.

3.4.2.4.90. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;

3.4.2.4.91. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:

3.4.2.4.92. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.4.2.4.93. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.

3.4.2.4.94. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;

3.4.2.4.95. Capacidade de limitar o acesso dos aplicativos a recursos do sistema, como chaves do registro e pastas/arquivos do sistema, por categoria, fabricante ou nível de confiança do aplicativo;

3.4.2.4.96. Capacidade de, em caso de epidemia, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web;

3.4.2.4.97. Capacidade de, caso o computador cliente saia da rede corporativa, ativar política alternativa onde qualquer configuração possa ser alterada, desde regras de firewall até controle de aplicativos, dispositivos e acesso à web.

3.4.2.4.98. Capacidade de voltar ao estado anterior do sistema operacional após um ataque de malware.

3.4.2.4.99. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

3.4.2.4.100. Capacidade de detectar anomalias no comportamento de um software,

usando análise heurística e aprendizado de máquina (machine learning).

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

3.4.2.4.102. Deve permitir realizar o gerenciamento por meio de integração via REST API.

3.4.2.4.103. Deve permitir o gerenciamento remoto da solução por meio de aplicativos de administração remota.

3.4.3. **Estações Mac OS X**

3.4.3.1. **Compatibilidade:**

3.4.3.1.1. macOS Mojave 10.14

3.4.3.1.2. macOS Catalina 10.15

3.4.3.1.3. macOS Big Sur 11.0

3.4.3.1.4. macOS Monterey 12

3.4.3.2. **Características:**

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

3.4.3.2.2. Possuir módulo de web-antivírus para proteger contra ameaças durante navegação na internet com possíbilidade de analisar endereços https;

3.4.3.2.3. Possuir módulo de bloqueio á ataques na rede;

3.4.3.2.4. Possibilidade de bloquear a comunicação entre a máquina atacante e os demais computadores por tempo definido pelo administrador;

3.4.3.2.5. Capacidade de criar exclusões para computadores que não devem ser monitorados pelo módulo de bloqueio à ataques na rede;

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

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

3.4.3.2.8. As vacinas devem ser atualizadas pelo fabricante e disponibilizada aos usuários de, no máximo, uma em uma hora independentemente do nível das ameaças encontradas no período (alta, média ou baixa);

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

3.4.3.2.10. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex:

"Win32.Trojan.banker") para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

3.4.3.2.11. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);

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

3.4.3.2.13. Capacidade de verificar somente arquivos novos e alterados;

3.4.3.2.14. Capacidade de verificar objetos usando heurística;

3.4.3.2.15. Capacidade de agendar uma pausa na verificação;

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

3.4.3.2.17. Perguntar o que fazer, ou;

3.4.3.2.18. Bloquear acesso ao objeto;

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

3.4.3.2.20. Caso positivo de desinfecção:

3.4.3.2.21. Restaurar o objeto para uso;

3.4.3.2.22. Caso negativo de desinfecção:

3.4.3.2.23. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

3.4.3.2.25. Capacidade de verificar arquivos de formato de email;

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

3.4.3.2.27. Capacidade de, através da mesma console central de gerenciamento:

3.4.3.2.28. Ser instalado;

3.4.3.2.29. Ser removido;

3.4.3.2.30. Ser gerenciado;

3.4.4. **Sistemas operacionais Linux**

3.4.4.1. **Compatibilidade:**

3.4.4.1.1. **Plataforma 32-bits:**

3.4.4.1.1.1. Red Hat Linux 6.7 e superior;

3.4.4.1.1.2. CentOS 6.7 e superior;

3.4.4.1.1.3. Debian 9.4 e superior;

3.4.4.1.1.4. Debian 10.1 e superior;

3.4.4.1.1.5. Debian 11.1 e superior;

3.4.4.2. **Plataforma 64-bits:**

3.4.4.2.1. Ubuntu 18.04 e superior;

3.4.4.2.2. Ubuntu 20.04;

3.4.4.2.3. Red Hat Enterprise Linux 8.0;

3.4.4.2.4. CentOS 8.0 e superior;

3.4.4.2.5. Debian 10.1 e superior;

3.4.4.2.6. Oracle Linux 8.0 e superior;

3.4.4.3. **Características:**

3.4.4.3.1. Deve prover as seguintes proteções:

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

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

3.4.4.3.4. Via linha de comando;

3.4.4.3.5. Via console administrativa;

3.4.4.3.6. Via GUI;

3.4.4.3.7. Via web (remotamente);

3.4.4.3.8. Deve possuir funcionalidade de scan de drives removíveis, tais como:

3.4.4.3.9. CDs;

3.4.4.3.10. DVDs;

3.4.4.3.11. Discos blu-ray;

3.4.4.3.12. Flash drives (pen drives);

3.4.4.3.13. HDs externos;

3.4.4.3.14. Disquetes;

3.4.4.3.15. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:

3.4.4.3.16. Por tipo de dispositivo;

3.4.4.3.17. Por barramento de conexão.

3.4.4.3.18. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

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

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

3.4.4.3.21. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

3.4.4.3.22. Leitura de configurações;

3.4.4.3.23. Modificação de configurações;

3.4.4.3.24. Gerenciamento de Backup;

3.4.4.3.25. Visualização de logs;

3.4.4.3.26. Gerenciamento de logs;

3.4.4.3.27. Gerenciamento de ativação da aplicação;

3.4.4.3.28. Gerenciamento de permissões (adicionar/excluir permissões acima);

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

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

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

3.4.4.3.32. Dectectar aplicações que possam ser utilizadas como vetor de ataque por hackers;

3.4.4.3.33. Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:

3.4.4.3.34. Alta;

3.4.4.3.35. Média;

3.4.4.3.36. Baixa;

3.4.4.3.37. Recomendado;

3.4.4.3.38. Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;

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

3.4.4.3.40. Em caso erros, deve ter capacidade de criar *logs* automaticamente, sem

necessidade de outros softwares;

3.4.4.3.41. Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;

3.4.4.3.42. Deverá ser possível priorizar a execução de tarefas;

3.4.4.3.43. Capacidade de verificar objetos usando heurística;

3.4.4.3.44. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;

3.4.4.3.45. Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;

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

3.4.4.3.47. Detecção de phishing e sites maliciosos;

3.4.4.3.48. Bloqueio de download de arquivos maliciosos;

3.4.4.3.49. Bloqueio de adware;

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

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

3.4.4.3.52. Deverá fornecer informações de todas os executáveis das aplicações;

3.4.4.3.53. Deve possuir módulo de proteção contra criptografia maliciosa.

3.4.4.3.54. Deverá possuir controle de execução de aplicações;

3.4.4.3.55. O modulo de controle de aplicação deverá possuir as seguintes funcionalidades:

3.4.4.3.56. Criação de lista de bloqueio de aplicação;

3.4.4.3.57. Criação de lista de permissão de aplicação;

3.4.4.3.58. Deverá realizar busca de ameaças em setores críticos do sistema operacional:

3.4.4.3.59. Setor de inicialização;

3.4.4.3.60. Objetos de inicialização;

3.4.4.3.61. Processos de memória;

3.4.4.3.62. Memória do kernel;

3.4.5. **Compatibilidade com servidores windows legados.**

3.4.5.1. **Compatibilidade de sistema legado:**

3.4.5.1.1. **Plataforma x32 ou x64:**

3.4.5.1.1.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;

3.4.5.1.1.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;

3.4.5.2. **Características:**

3.4.5.2.1. Deve prover as seguintes proteções:

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

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

3.4.5.2.4. Firewall com IDS;

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

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

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

3.4.5.2.8. Via console administrativa;

3.4.5.2.9. Via web (remotamente);

3.4.5.2.10. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;

3.4.5.2.11. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.

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

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

3.4.5.2.14. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);

3.4.5.2.15. Leitura de configurações;

3.4.5.2.16. Modificação de configurações;

3.4.5.2.17. Gerenciamento de backup;

3.4.5.2.18. Visualização de logs;

3.4.5.2.19. Gerenciamento de logs;

3.4.5.2.20. Gerenciamento de ativação da aplicação;

3.4.5.2.21. Gerenciamento de permissões (adicionar/excluir permissões acima);

3.4.5.2.22. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.

3.4.5.2.23. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:

3.4.5.2.24. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;

3.4.5.2.25. Filtragem por aplicativo: onde o administrador poderá escolher qual aplicativo, grupo de aplicativo, fabricante de aplicativo, versão de aplicativo ou nome de aplicativo terá acesso a rede, com a possibilidade de escolher quais portas e protocolos poderão ser utilizados.

3.4.5.2.26. Capacidade de separadamente selecionar o número de processos que irão executar funções de varredura em tempo real, o número de processos que executarão a varredura sob demanda e o número máximo de processos que podem ser executados no total;

3.4.5.2.27. Bloquear malwares tais como Cryptlockers mesmo quando o ataque vier de um computador sem antivírus na rede

3.4.5.2.28. Capacidade de resumir automaticamente tarefas de verificação que tenham sido paradas por anormalidades (queda de energia, erros, etc);

3.4.5.2.29. Em caso de erros, deve ter capacidade de criar *logs* e *traces* automaticamente, sem necessidade de outros softwares;

3.4.5.2.30. Deve possuir funcionalidade de análise personalizada de logs do Windows.

3.4.5.2.31. Capacidade de configurar níveis de verificação diferentes para cada pasta, grupo de pastas ou arquivos do servidor;

3.4.5.2.32. Capacidade de bloquear acesso ao servidor de máquinas infectadas e quando uma máquina tenta gravar um arquivo infectado no servidor;

3.4.5.2.33. Capacidade de criar uma lista de máquina que nunca serão bloqueadas mesmo quando infectadas;

3.4.5.2.34. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;

3.4.5.2.35. Capacidade de adicionar pastas/arquivos para uma zona de exclusão, a fim de excluí-los da verificação. Capacidade, também, de adicionar objetos a lista de exclusão de acordo com o veredicto do antivírus, (ex: “Win32.Trojan.banker”) para que qualquer objeto detectado com o veredicto escolhido seja ignorado;

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

da extensão do arquivo;

3.4.5.2.37. Capacidade de verificar somente arquivos novos e alterados;

3.4.5.2.38. Capacidade de escolher qual tipo de objeto composto será verificado (ex: arquivos comprimidos, arquivos auto descompressores, .PST, arquivos compactados por compactadores binários, etc.);

3.4.5.2.39. Capacidade de verificar objetos usando heurística;

3.4.5.2.40. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

3.4.5.2.41. Capacidade de agendar uma pausa na verificação;

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

3.4.5.2.43. Perguntar o que fazer, ou;

3.4.5.2.44. Bloquear acesso ao objeto;

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

3.4.5.2.46. Caso positivo de desinfecção:

3.4.5.2.47. Restaurar o objeto para uso;

3.4.5.2.48. Caso negativo de desinfecção:

3.4.5.2.49. Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);

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

3.4.5.2.51. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos malicioso em área de backup;

3.4.5.2.52. Possibilidade de escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;

3.4.5.2.53. Em caso de detecção de sinais de de uma infecção ativa, deve possuir capacidade de, automaticamente:

3.4.5.2.54. Executar os procedimentos pré-configurados pelo administrador;

3.4.5.2.55. Em caso de ausência de procedimentos pré-configurados, criar tais procedimentos e executá-los.

3.4.5.2.56. Deve possuir módulo que analise cada script executado, procurando por sinais de atividade maliciosa.

3.4.5.2.57. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

3.4.5.2.58. Capacidade de detectar anomalias no comportamento de um software usando análise heurística.

3.4.5.2.59. Capacidade de bloquear a criptografia de arquivos em pastas compartilhadas, após a execução de um malware em um dispositivo que possua o mapeamento da pasta.

3.4.5.2.60. Deve possuir controle de dispositivos externos.

3.4.6. **Smartphones e tablets**

3.4.6.1. **Compatibilidade com Android**

3.4.6.1.1. Android das versões: 5.0 ao 12.

3.4.6.2. **Características:**

3.4.6.2.1. Deve prover as seguintes proteções:

3.4.6.2.2. Proteção em tempo real do sistema de arquivos do dispositivo – interceptação e verificação de:

3.4.6.2.3. Proteção contra adware e autodialers;

3.4.6.2.4. Todos os objetos transmitidos;

3.4.6.2.5. Arquivos abertos no smartphone;

3.4.6.2.6. Programas instalados usando a interface do smartphone

3.4.6.2.7. Verificação dos objetos na memória interna do smartphone e nos cartões de expansão sob demanda do usuário e de acordo com um agendamento;

3.4.6.2.8. Deverá isolar em área de backup os arquivos infectados;

3.4.6.2.9. Deverá atualizar as bases de vacinas de modo agendado;

3.4.6.2.10. Capacidade de desativar por política:

3.4.6.2.11. Wi-fi;

3.4.6.2.12. Câmera;

3.4.6.2.13. Bluetooth.

3.4.6.2.14. Deverá ter função de limpeza de dados pessoais a distância, em caso de roubo, por exemplo;

3.4.6.2.15. Capacidade de requerer uma senha para desbloquear o dispositivo e personalizar a quantidade de caracteres para esta senha;

3.4.6.2.16. Deverá ter firewall pessoal;

3.4.6.2.17. Capacidade de tirar fotos quando a senha for inserida incorretamente;

3.4.6.2.18. Capacidade de enviar comandos remotamente de:

3.4.6.2.19. Localizar;

3.4.6.2.20. Bloquear.

3.4.6.2.21. Capacidade de detectar Root nos dispositivos;

3.4.6.2.22. Capacidade de bloquear o acesso a site por categoria em dispositivos;

3.4.6.2.23. Capacidade de bloquear o acesso a sites phishing ou maliciosos;

3.4.6.2.24. Capacidade de configurar White e blacklist de aplicativos;

3.4.6.2.25. Capacidade de localizar o dispositivo quando necessário;

3.4.6.2.26. Permitir atualização das definições quando estiver em "roaming";

3.4.6.2.27. Capacidade de selecionar endereço do servidor para buscar a definição de vírus;

3.4.6.2.28. Capacidade de agendar uma verificação;

3.4.6.2.29. Capacidade de enviar URL de instalação por e-mail;

3.4.6.2.30. Capacidade de fazer a instalação do agente através de um link QRCode;

3.4.6.2.31. Capacidade de executar as seguintes ações caso a desinfecção falhe:

3.4.6.2.32. Deletar;

3.4.6.2.33. Ignorar;

3.4.6.2.34. Fazer backup;

3.4.6.2.35. Perguntar ao usuário.

3.4.7. **Compatibilidade com iOS:**

3.4.7.1. **Ser compatível com disposiitivos com os sistemas operacionais:**

3.4.7.1.1. iOS 10.0 – 10.3.3

3.4.7.1.2. iOS 11.0 – 11.3

3.4.7.1.3. iOS 12.0

3.4.7.1.4. iOS 13.0

3.4.7.1.5. IPadOS 13 ao 15

3.4.7.2. **Características:**

3.4.7.2.1. Capacidade de ajustar as configurações de:

3.4.7.2.2. Senha do usuário;

3.4.7.2.3. Criptografia de dados;

3.4.7.2.4. Capacidade de instalar certificados digitais em dispositivos móveis;

3.4.7.2.5. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:

3.4.7.2.6. Link por e-mail;

3.4.7.2.7. Link por mensagem de texto;

3.4.7.2.8. QR Code

3.4.7.2.9. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;

3.4.7.2.10. Capacidade de, remotamente, bloquear um dispositivo iOS;

3.4.8. **Criptografia**

3.4.8.1. **Compatibilidade**

3.4.8.1.1. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;

3.4.8.1.2. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;

3.4.8.1.3. Microsoft Windows 7 Professional SP1 ou superior x86/x64;

3.4.8.1.4. Microsoft Windows 8 Enterprise x86/x64;

3.4.8.1.5. Microsoft Windows 8 Pro x86/x64;

3.4.8.1.6. Microsoft Windows 8.1 Pro x86/x64;

3.4.8.1.7. Microsoft Windows 8.1 Enterprise x86/x64;

3.4.8.1.8. Microsoft Windows 10 Enterprise x86/x64;

3.4.8.1.9. Microsoft Windows 10 Pro x86/x64;

3.4.9. **Características:**

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

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

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

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

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

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

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

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

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

3.4.9.10. Criptografar todos os arquivos individualmente;

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

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

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

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

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

3.4.9.16. Verifica compatibilidade de hardware antes de aplicar a criptografia;

3.4.9.17. Possibilita estabelecer parâmetros para a senha de criptografia;

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

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

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

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

3.4.9.22. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;

3.4.9.23. Permite criar um grupo de extensões de arquivos a serem criptografados;

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

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

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

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

3.4.9.28. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;

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

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

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

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

3.4.9.33. Capacidade de fazer “Hardware encryption”;

3.4.10. **Gerenciamento de Sistemas**

3.4.10.1. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;

3.4.10.2. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;

3.4.10.3. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;

3.4.10.4. Capacidade de corrigir as vulnerabilidades de softwares, fazendo o download centralizado da correção ou atualização e aplicando essa correção ou atualização nas máquinas gerenciadas de maneira transparente para os usuários;

3.4.10.5. Capacidade de gerenciar licenças de softwares de terceiros;

3.4.10.6. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;

3.4.10.7. Possibilita fazer distribuição de software de forma manual e agendada;

3.4.10.8. Suporta modo de instalação silenciosa;

3.4.10.9. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;

3.4.10.10. Possibilita fazer a distribuição através de agentes de atualização;

3.4.10.11. Utiliza tecnologia multicast para evitar tráfego na rede;

3.4.10.12. Possibilita criar um inventário centralizado de imagens;

3.4.10.13. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;

3.4.10.14. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;

3.4.10.15. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;

3.4.10.16. Capacidade de gerar relatórios de vulnerabilidades e patches;

3.4.10.17. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;

3.4.10.18. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;

3.4.10.19. Permite baixar atualizações para o computador sem efetuar a instalação

3.4.10.20. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações

incluindo as bloqueadas;

3.4.10.21. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;

3.4.10.22. Permite selecionar produtos a serem atualizados pela console de gerenciamento;

3.4.10.23. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;

3.4.10.24. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;

3.4.10.25. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;

3.4.10.26. Capacidade de configurar o reinicio do computador após a aplicação das atualizações e correções de vulnerabilidades;

3.4.10.27. Deve permitir selecionar o idioma das aplicações que serão atualizadas;

3.4.10.28. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

3.4.11. **Detecção e Resposta**

3.4.11.1. **Compatibilidade**

3.4.11.1.1. Deve ser compatível com os seguintes sistemas de estação de trabalho:

3.4.11.1.1.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

3.4.11.1.1.2. Microsoft Windows 8 Professional/Enterprise;

3.4.11.1.1.3. Microsoft Windows 8.1 Professional / Enterprise;

3.4.11.1.1.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;

3.4.11.1.1.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;

3.4.11.1.2. Deve ser compatível com os seguintes sistemas servidores:

3.4.11.1.2.1. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;

3.4.11.1.2.2. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;

3.4.11.1.2.3. Windows Server 2016 Essentials / Standard / Datacenter;

3.4.11.1.2.4. Windows Server 2019 Essentials / Standard / Datacenter;

3.4.11.1.2.5. Windows Server 2022.

3.4.11.2. **Características:**

3.4.11.2.1. As funcionalidades relacionadas a detecção e resposta solicitadas nesse item, devem ser operadas na mesma console de gerenciamento da solução de endpoint;

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

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

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

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

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

3.4.11.2.7. Isolar o host;

3.4.11.2.8. Iniciar uma varredura nas áreas críticas;

3.4.11.2.9. Quarentenar o objeto;

3.4.11.2.10. A solução deve criar um report detalhado sobre o incidente, tendo a capacidade de incluir no mínimo os seguintes dados:

3.4.11.2.11. Visibilidade das detecções provenientes de endpoint;

3.4.11.2.12. Processos;

3.4.11.2.13. Conexões remotas;

3.4.11.2.14. Alterações de registros;

3.4.11.2.15. Objetos baixados

3.4.11.2.16. Capacidade de integração com a solução de sandbox cloud do fabricante;

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

3.4.11.2.18. Deverá possuir informações de assinaturas digitais da ameaça;

3.4.11.2.19. Deve ser capaz de trazer informações do arquivo sobre sua geolocalização;

3.4.11.2.20. Possibilidade de informar quando o arquivo foi detectado pela base de conhecimento;

3.4.11.2.21. Trazer a identificação de comportamento e/ou descrição sobre o arquivo;

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

3.4.11.2.23. Prevenir a execução de um arquivo;

3.4.11.2.24. Quarentenar um arquivo;

3.4.11.2.25. Iniciar uma varredura por IoC;

3.4.11.2.26. Parar um processo;

3.4.11.2.27. Executar um processo;

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

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

3.4.11.2.30. Na análise do incidente a ferramenta deverá apresentar recomendações de ações que o analista precisa executar para remediar o incidente;

3.4.11.2.31. As recomendações devem ser guiadas juntamente com guias das opções selecionadas pelo analista, apresentando pop-up guiando as ações.

3.4.11.2.32. Deverá ser possível remover a máquina do isolamento a partir do incidente;

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

3.4.11.2.34. Deve oferecer informações de inteligência de ameaças do próprio fabricante;

3.4.11.2.35. Deverá possuir detecção baseada em sandbox do tipo cloud;

3.4.11.2.36. Deverá suportar IoC de terceiros em formatos OpenIOC.

3.4.12. Especificação técnica mínima Solução de Segurança de EndPoint XDR

3.4.12.1. A solução XDR deve atender a todas as especificações previamente mencionadas para EDR, além de incorporar as seguintes funcionalidades adicionais:

3.4.12.2. Console do módulo de detecção e reposta.

3.4.12.2.1. Console de gerenciamento deve apresentar uma dashboard customizável.

3.4.12.2.2. Deve apresentar a saúde do sistema, informando quais componentes estão atualizados ou não.

3.4.12.2.3. Deve permitir criar perfis de layout;

3.4.12.2.4. Deve permitir exportar para PDF o layout atual da solução;

3.4.12.2.5. Deve mostrar pelo menos as seguintes informações atualizadas sobre a ferramenta:

3.4.12.2.5.1. Saúde do sistema;

3.4.12.2.5.2. Tráfego em tempo real;

3.4.12.2.5.3. Mostrar alertas por importância;

3.4.12.2.5.4. Alertas por tecnologias de detecção;

3.4.12.2.5.5. Alertas por vetor de ataques;

3.4.12.2.5.6. Deve permitir criar novos usuários para acesso à console com pelo menos 3 níveis de acesso.

3.4.12.2.6. Deve permitir integração com a Console de gerenciamento da ferramenta de antimalware;

3.4.12.2.7. Deve mostrar quantidades de eventos pela criticidade, alto, médio ou baixo;

3.4.12.2.8. Possibilidade de assinalar um evento para determinado usuário para verificação;

3.4.12.2.9. Deve suportar arquivos no formato CEF para integração com SIEM;

3.4.12.2.10. O usuário com conta de administrador de segurança deve ter permissão para assinalar um incidente para usuários específicos;

3.4.12.2.11. Possibilidade de marcar evento como processado para informar que o incidente já foi analisado e resolvido;

3.4.12.2.12. Deve se possível gerenciar o status de cada evento;

3.4.12.2.13. As seguintes informações devem ser mostradas nos alertas de eventos:

3.4.12.2.13.1. Status do Alerta.

3.4.12.2.13.2. Nível de importância.

3.4.12.2.13.3. Servidor em que o alerta foi criado.

3.4.12.2.13.4. Host em que ocorreu o ataque.

3.4.12.2.13.5. Fonte dos dados.

3.4.12.2.13.6. Hora em que o alerta foi criado.

3.4.12.2.13.7. Hora em que as informações do alerta foram atualizadas.

3.4.12.2.13.8. Nome do arquivo.

3.4.12.2.13.9. Tipo de arquivo.

3.4.12.2.13.10. Tamanho do arquivo.

3.4.12.2.13.11. Hash MD5 e 256 do arquivo.

3.4.12.2.13.12. E-mail.

3.4.12.2.13.13. Assunto do e-mail.

3.4.12.2.13.14. IP do Servidor de envio.

3.4.12.2.13.15. Cabeçalho.

3.4.12.2.13.16. Objetos Detectados.

3.4.12.2.13.17. URL.

3.4.12.2.13.18. Usuário.

3.4.12.2.13.19. Tecnologia e módulos que detectaram a ameaça.

3.4.12.2.14. Deve permitir importar IOCs (Indices de comprometimento) visando encontrar ataques de acordo com informações contidas no IoC;

3.4.12.2.15. Capacidade de executar as seguintes tarefas remotamente nos endpoints:

3.4.12.2.15.1. Finalizar processo;

3.4.12.2.15.2. Executar programa;

3.4.12.2.15.3. Coletar arquivo;

3.4.12.2.15.4. Deletar arquivo;

3.4.12.2.15.5. Quarentenar arquivo;

3.4.12.2.15.6. Restaurar arquivo da quarentena;

3.4.12.2.16. Deve permitir ao coletar um arquivo remotamente enviar automaticamente para o SANDBOX para análise;

3.4.12.2.17. Deve possuir funcionalidade que permita prevenir um arquivo de ser executado através do hash MD5/SHA256;

3.4.12.2.18. Deverá possuir capacidade de disponibilizar facilmente as amostras dos arquivos suspeitos detectados e do arquivo PCAP do contexto de captura;

3.4.12.2.19. Deverá permitir o uso de base de conhecimento na Internet do próprio fabricante, com atualização automática de regras e assinaturas, para consultas automáticas em bases de reputação e correlacionamento de informações sobre ameaças conhecidas, identificando assim as respectivas recomendações de ações;

3.4.12.2.20. Deve possuir plataforma de inteligência de ameaças, informando se o ataque faz parte de uma campanha global, quais as regiões e plataformas afetadas pelo ataque, bem como disponibilizar links de referência sobre a ameaça;

3.4.12.2.21. Deve possuir plataforma do próprio fabricante com informações sobre as ameaças, informando título, data descoberta e descrição sobra a ameaça.

3.4.12.2.22. Deve possuir integração com portal de inteligência para avançar na pesquisa a partir dos eventos;

3.4.12.2.23. Deve ser possível realizar consultas de IP, HASH domínios no portal de

inteligência do próprio fabricante.

3.4.12.2.24. Para cada malware, exploit ou componente malicioso, a ferramenta deve possuir links para detalhar informações sobre estes;

3.4.12.2.25. Possibilidade de selecionar quais dispositivos serão afetados pela tarefa de prevenção de execução de arquivos;

3.4.12.2.26. Capacidade de baixar arquivos quarentenados diretamente pela console de administração;

3.4.12.2.27. Deve mostrar quantos Endpoints estão sendo gerenciados informando detalhes sobre sua atividade, tais como: Inatividade, desatualizados e hosts sincronizados;

3.4.12.2.28. Possuir relatórios customizáveis possibilitando adicionar ou remover colunas de identificação e status de eventos;

3.4.12.2.29. Deve permitir criar relatórios baseados na tecnologia de proteção utilizada;

3.4.12.2.30. Criar relatórios de eventos organizados pelas seguintes severidades: baixa, média e alta;

3.4.12.2.31. Deve permitir adicionar imagens ao relatório;

3.4.12.2.32. Permitir criar listas brancas baseadas nos seguintes filtros:

3.4.12.2.32.1. Por hash MD5;

3.4.12.2.32.2. Por formato;

3.4.12.2.32.3. Por URL;

3.4.12.2.32.4. Por e-mail;

3.4.12.2.32.5. Por subrede;

3.4.12.2.33. Permitir criar regras de notificações para envio por e-mail quando novos eventos são identificados pela ferramenta;

3.4.12.2.34. Deve permitir configurar o status do endpoint de acordo com a quantidade de dias de inatividade;

3.4.12.2.35. Deve permitir integrar com solução de SIEM por protocolo de syslog, através de encriptação usando TLS.

3.4.12.3. Módulo de Sandbox

3.4.12.3.1. As Sandboxes deverão suportar os seguintes sistemas operacionais:

3.4.12.3.1.1. Windows XP x86 Sp3;

3.4.12.3.1.2. Windows 7 X64;

3.4.12.3.1.3. Windows 10 x64;

3.4.12.3.1.4. CentOS 7.8.

3.4.12.3.2. Suportar atualização da base de dados da Rede de Inteligência de forma automática e sem causar nenhum tipo de indisponibilidade da solução.

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

3.4.12.3.4. A solução deve ser capaz de prover dados forense detalhados, via interface gráfica, relacionados à infecção, demonstrando o ciclo de vida completo do ataque. Estes dados forenses devem incluir a cronologia completa do ataque e não apenas uma porção do ataque, assim como:

3.4.12.3.4.1. URLs/sites web relacionados ao ataque,

3.4.12.3.4.2. hashes MD5

3.4.12.3.5. Detectar e inspecionar, no mínimo, os seguintes tipos de arquivo, considerando as diferentes versões de sistemas operacionais e aplicativos existentes:

3.4.12.3.6. Arquivos executáveis;

3.4.12.3.7. Scripts;

3.4.12.3.8. Arquivos;

3.4.12.3.9. Documentos do office;

3.4.12.3.10. Arquivos de mídia;

3.4.12.3.11. Arquivos de Android (APK)

3.4.12.3.12. A solução deve suportar importação de regras YARA personalizadas, para permitir flexibilidade na criação de regras para análise de ameaças;

3.4.12.3.13. Suportar mecanismo de whitelist pelos seguintes métodos:

3.4.12.3.13.1. Hash MD5 do arquivo;

3.4.12.3.13.2. Formato do arquivo;

3.4.12.3.13.3. E-mail;

3.4.12.3.13.4. Subrede.

3.4.12.3.13.5. Deve permitir o envio de alertas por e-mail;

3.4.12.3.14. Deverá possuir a capacidade de detectar ameaças direcionadas, realizando inspeção de tráfego até a camada 7 de forma a prevenir ataques do dia zero e executar análise profunda de documentos que contenham conteúdo malicioso ou redirecionamentos para outras URL's maliciosas;

3.4.12.3.15. Capacidade de instalar imagens customizadas do Windows para analisar

objetos na Sandbox.

3.5. Garantia e suporte técnico

3.5.1. Durante 60 (sessenta) meses, a Contratada deverá prover a garantia, manutenção e suporte técnico.

3.5.2. Durante a vigência da garantia e suporte técnico, a Contratada deverá fornecer, sem custos adicionais para o TJCE, novas versões da solução, incluindo correções de falhas (bugs) na aplicação, atualizações de proteção das ameaças e melhorias para as licenças adquiridas.

3.5.3. Os serviços de suporte devem abranger ações corretivas, proativas e consultivas, englobando tarefas como assistência na configuração de políticas e administração da solução, implantação de novas versões, patches e hotfixes, esclarecimento de dúvidas sobre melhores práticas de configuração, entre outras.

3.5.4. A Contratada deve fornecer Suporte Técnico e Especializado para resolver questões relacionadas ao funcionamento das soluções e das licenças/agentes instalados em computadores (endpoints e servidores) e pela manutenção da plataforma de gerenciamento.

3.5.5. O suporte pode ser prestado de forma presencial ou remota.

3.5.6. O Suporte Técnico engloba as seguintes atividades:

3.5.6.1. Identificação e resolução de falhas na solução.

3.5.6.2. Assistência na instalação de licenças/agentes.

3.5.6.3. Auxílio na operação da console de gerenciamento.

3.5.6.4. Abordagem de problemas de disponibilidade dos serviços contratados.

3.5.6.5. Qualquer outro suporte relacionado aos serviços contratados.

3.5.7. A Contratada deve fornecer todas as atualizações de versões que ocorrerem durante o período de vigência das licenças.

3.5.8. Informações sobre os canais de atendimento para abrir chamados devem ser comunicadas à Contratante durante a reunião inicial, após a assinatura do contrato e a emissão da ordem de serviço.

3.5.9. É obrigatório que a Contratada registre todas as solicitações de suporte técnico, independentemente de sua natureza, e a Contratante deve acompanhar esses registros.

3.5.10. O Suporte Técnico deve ser realizado por técnicos especializados e certificados pelo fabricante da solução.

3.5.11. A resolução de um chamado é medida pelo tempo total decorrido desde a abertura até a solução definitiva do problema.

3.5.12. A Contratada deverá disponibilizar canais para a abertura de chamados, como uma central de atendimento ao custo de uma ligação local, e também disponibilizar e-mail ou sistema web para atender às solicitações de suporte do TJCE e para acompanhamento de chamados abertos.

3.5.13. O suporte técnico prestado pela Contratada deverá ser realizado em língua portuguesa, sem a necessidade de intérpretes, e deve garantir prazos de atendimento 24 horas por dia, 7 dias por semana.

3.5.14. Nos chamados registrados, deverão ser registrados, no mínimo, os seguintes dados:

3.5.14.1. Data e hora da abertura do chamado.

3.5.14.2. Identificação do requisitante da abertura do chamado.

3.5.14.3. Identificação do número do contrato.

3.5.14.4. Descrição do serviço/ocorrência.

3.5.14.5. Identificação da severidade do serviço/ocorrência.

3.5.14.6. Identificação do atendente da Contratada responsável pelo registro do chamado.

3.5.15. O suporte técnico deve compreender a prestação de assistência por meio de acesso remoto à rede do TJCE, sempre que for necessário realizar procedimentos e configurações técnicas para assegurar o uso apropriado e otimizado da solução.

3.5.16. Para fins de suporte técnico, os seguintes critérios serão considerados:

3.5.16.1. Prazo de Atendimento inicial: Esse prazo é o intervalo de tempo entre a abertura do chamado técnico realizado pelo TJCE na Central de Atendimento da Contratada e o início efetivo dos trabalhos de suporte.

3.5.16.2. Prazo de Solução Definitiva: Esse prazo representa o período decorrido desde a abertura do chamado técnico feito pelo TJCE na Central de Atendimento da Contratada até a completa restauração da solução ao pleno funcionamento.

3.5.17. O prazo de solução pode ser estendido, desde que haja uma prévia aprovação do Fiscal Técnico do Contrato, conforme as condições acordadas durante o atendimento.

3.5.18. Em situações devidamente comprovadas em que a resolução da solução dependa exclusivamente do fabricante, a prorrogação do prazo pode ocorrer, seguindo as definições estabelecidas entre os fiscais e a empresa Contratada.

3.5.19. O suporte técnico da Contratada deve atender os seguintes níveis de serviço, conforme descrito a seguir:

SEVERIDADE	DESCRIÇÃO	TEMPO DE ATENDIMENTO INICIAL	TEMPO MÁXIMO PARA SOLUÇÃO DEFINITIVA
Severidade 1	Solução antivírus inoperante.	Até 1 hora.	8 horas.
Severidade 2	Solução antivírus funcionando de forma intermitente e/ou com limitações.	Até 3 horas.	24 horas.
Severidade 3	Solução antivírus com registros de mau funcionamento, porém sem impacto significativo no ambiente da TJCE.	Até 6 horas.	48 horas.
Severidade 4	Dúvidas e/ou necessidade de esclarecimentos técnicos para a utilização adequada e otimizada da solução antivírus.	Até 48 horas.	96 horas.

3.5.20. No caso de ocorrências com severidade 1, a Contratada deverá apresentar uma solução paliativa ou definitiva em até 1 (uma) hora após o primeiro atendimento.

3.5.21. A severidade do problema será determinada pelo TJCE no momento da abertura do chamado.

3.5.22. A cada problema relatado, será aberto um chamado técnico, e a contagem do tempo de atendimento começará no momento do acionamento.

3.5.23. Todas as despesas decorrentes do suporte remoto ou presencial desses atendimentos serão de responsabilidade da Contratada.

3.5.24. Para calcular o tempo gasto pela Contratada na disponibilização da solução, os períodos em que o TJCE for responsável por executar ações necessárias para analisar e resolver a ocorrência não serão considerados.

3.5.25. Não deve haver restrições quanto ao número de colaboradores do TJCE autorizados a iniciar chamados de suporte técnico.

3.5.26. O suporte técnico, manutenção e garantia devem ser fornecidos pelo fabricante ou por sua rede credenciada formalmente autorizada.

3.5.27. As manutenções realizadas devem abranger apenas o conjunto de ferramentas que compõem a solução, não devendo afetar nenhum outro ambiente de sistema ou rede do TJCE.

3.5.28. No contexto de atendimentos remotos, a Contratada deve notificar o fiscal técnico do contrato via e-mail tanto no início quanto na conclusão desses atendimentos, fornecendo evidências das atividades realizadas.

3.5.29. Na conclusão do suporte técnico, a Contratada informará o andamento dos trabalhos ao Fiscal Técnico e requererá a devida autorização para o encerramento do chamado. Se, porventura, o Fiscal Técnico não endossar a completa solução definitiva do problema, o chamado será mantido em aberto até que a Contratada efetivamente resolva a questão. Em tal cenário, o Fiscal Técnico relatará as pendências associadas ao chamado que permanece em aberto.

3.5.30. Em todos os cenários que demandem tal ação e quando se mostrar pertinente, a Contratada está obrigada a transmitir informações relativas às correções a serem implementadas ou as próprias correções, via mensagens de correio eletrônico destinada aos fiscais técnicos.

3.5.31. No evento em que não ocorra qualquer pronunciamento por parte da Contratada no lapso temporal determinado na tabela de severidade, ou se o Fiscal do Contrato venha a considerar insatisfatória a justificativa apresentada, será instaurado um procedimento de sugestão para a aplicação das sanções previstas.

3.5.32. O descumprimento de um ou mais indicadores de nível de serviço resultará na aplicação de notificação ou penalidade à Contratada.

3.5.33. O TJCE avaliará as justificativas fundamentadas apresentadas pela Contratada para a não aplicação das notificações ou penalidades.

3.5.34. Após a avaliação, o Fiscal do Contrato comunicará à Contratada a quantidade de ocorrências registradas durante o período em questão.

3.5.35. A Contratada terá um prazo de 5 (cinco) dias úteis para apresentar contestação e as devidas justificativas para a ocorrência registrada.

3.5.36. As justificativas da Contratada somente serão aceitas se a excepcionalidade da ocorrência for comprovada.

3.6. Treinamento

3.6.1. A Contratada deverá disponibilizar um total mínimo de 8 (oito) vagas para treinamento da solução.

3.6.2. O Treinamento deverá ser oficial abrangendo todas as funcionalidades da solução com a carga horária mínima de 24 (vinte e quatro) horas.

3.6.3. O treinamento será realizado de forma online ou presencial, em turmas fechadas com um máximo de 10 alunos por instrutor certificado pela fabricante da solução.

3.6.4. O treinamento atenderá a todos os requisitos necessários, incluindo o uso de laboratórios virtuais e outras ferramentas essenciais.

3.6.5. Para a inscrição dos funcionários que participarão do treinamento, o TJCE deverá fornecer à Contratada os nomes e e-mails dos participantes.

3.6.6. O treinamento será ministrado em idioma português.

3.6.7. O material didático deverá ser disponibilizado, preferencialmente, em língua portuguesa.

3.6.8. O treinamento deverá capacitar os participantes na administração e operação eficiente da solução adquirida.

3.6.9. Ao término do treinamento, os participantes deverão receber um certificado de conclusão.

3.6.10. No caso de treinamento presencial, este deverá ser realizado no município de Fortaleza. Caso ocorra em outro local, todos os custos relativos a transporte, hospedagem e alimentação serão de responsabilidade da Contratada.

3.7. Implantação

3.7.1. A Contratada deverá elaborar e submeter para aprovação o Plano de Instalação da solução, o qual compreenderá o planejamento dos seguintes aspectos:

3.7.1.1. Implantação da Solução de Segurança de EndPoint EDR/XDR, garantindo que essa ação não afete a operação da rede atual e minimize os riscos de segurança durante a atualização do antivírus.

3.7.1.2. Instalação e configuração do software de gerenciamento da solução.

3.7.1.3. Criação de regras e grupos, estruturados de acordo com as melhores práticas de segurança e alinhados com as diretrizes estabelecidas pela equipe técnica do TJCE.

3.7.1.4. Instalação do software agente nos dispositivos endpoints.

3.7.2. A Contratada será responsável pela instalação e configuração do Servidor de administração e console de gerenciamento, seja na infraestrutura da Contratante ou na nuvem do fabricante.

3.7.3. A Contratada deverá realizar os seguintes serviços:

3.7.3.1. Implementação, configuração e implantação completa da solução, incluindo a transferência de conhecimentos relacionados à operacionalização das ferramentas da solução.

3.7.3.2. Transferência de conhecimento operacional abrangendo todas as funcionalidades da solução para a equipe técnica da Contratante.

3.7.3.3. Configuração das regras de segurança e grupos, aderindo às melhores práticas de segurança e seguindo as diretrizes previamente definidas pela equipe técnica da Contratante.

3.7.3.4. Implantação do software agente nos dispositivos endpoints, seguindo o planejamento estabelecido pela equipe técnica da Contratante e em conformidade com o Plano de Instalação aprovado.

4. MODELO DE EXECUÇÃO DO OBJETO

4.1. Após a formalização do contrato, será agendada uma reunião inicial de alinhamento como primeiro passo do processo de implementação, em até 10 (dez) dias corridos contados após a assinatura do contrato.

4.1.1. O propósito da reunião inicial é providenciar o planejamento da implantação e promover a transferência de conhecimento das ferramentas da solução e do ambiente de

rede do TJCE.

4.2. A execução do objeto seguirá a seguinte dinâmica:

4.2.1. **Entrega das licenças.**

4.2.1.1. A contratada deverá disponibilizar as licenças de uso de software em sítio oficial do fabricante, conforme descritivo técnico especificado no item 3.4, no prazo máximo de 30 (trinta) dias corridos a partir do recebimento da Ordem de Serviço das soluções contratadas identificadas em 1 e 2 no item 1.2.

4.2.1.2. Após a entrega das licenças, o TJCE emitirá um **Termo de Recebimento Provisório (TRP)** e em até 5 (cinco) dias úteis validará as licenças, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Caso a validação indique pendências, a Contratada deverá executar as retificações em até 15 (quinze) dias corridos.

4.2.1.3. Após a validação sem pendências da disponibilização das licenças, será assinado o **Termo de Recebimento Definitivo (TRD)** de entrega das licenças, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Somente a partir da assinatura do TRD, a execução dos serviços será considerada finalizada para finalidade de pagamento.

4.2.2. **Implantação.**

4.2.2.1. A Contratada deverá implantar a solução, no prazo máximo de 90 (noventa) dias corridos a partir do recebimento da Ordem de Serviço de implantação contratada identificado em 3 no item 1.2. com todos os requisitos descritos no item 3.7 atendidos e documentados em um relatório de implantação.

4.2.2.2. Após a implantação, o TJCE emitirá um **Termo de Recebimento Provisório (TRP)** e em até 5 (cinco) dias úteis validará a implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Caso a validação indique pendências de implantação, a Contratada deverá executar as retificações em até 15 (quinze) dias corridos.

4.2.2.3. Após a validação sem pendências da implantação, será assinado o **Termo de Recebimento Definitivo (TRD)** de implantação, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Somente a partir da assinatura do TRD, a execução dos serviços será considerada finalizada para finalidade de pagamento.

4.2.3. **Treinamento.**

4.2.3.1. A Contratada deverá realizar o serviço de treinamento, especificado no item

3.6, no prazo máximo de 90 (noventa) dias corridos a partir do recebimento da Ordem de Serviço.

4.2.3.2. Após ser ministrado o treinamento, o TJCE emitirá um **Termo de Recebimento Provisório (TRP)** e em até 5 (cinco) dias úteis validará o treinamento, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Caso a validação indique pendências no treinamento, a Contratada deverá executar as retificações em até 15 (quinze) dias corridos.

4.2.3.3. Após a validação sem pendências do treinamento, será assinado o **Termo de Recebimento Definitivo (TRD)** do treinamento, em conformidade com o estabelecido no Art. 140, da Lei 14.133/2021. Somente a partir da assinatura do TRD, a execução dos serviços será considerada finalizada para finalidade de pagamento.

4.2.4. Se, a qualquer momento, for constatado que o serviço ou software foi fornecido em desacordo com as especificações Contratadas, ocasionando mau funcionamento da solução, a responsabilidade pela reparação ou, se necessário, pela substituição recai integralmente sobre a Contratada. Diante de quaisquer problemas, a Contratada dispõe de um prazo fixo de 10 (dez) dias corridos, contados a partir da notificação, para efetuar quaisquer correções, ajustes ou substituições no objeto do contrato.

4.2.5. No caso de o serviço ou software fornecido não atender às especificações ou apresentar quaisquer defeitos, tais elementos serão considerados não entregues, e a contagem do prazo de entrega estipulado não será interrompida em decorrência da rejeição, impondo à Contratada todas as responsabilidades e ônus decorrentes desse atraso, passíveis de sanções contratuais.

4.2.6. Salienta-se que o aceite e o subsequente pagamento dos softwares/serviços por parte do TJCE não isentam a Contratada de suas obrigações para correção de quaisquer defeitos, falhas ou outras irregularidades no objeto contratado.

5. MODELO DE GESTÃO DO CONTRATO

5.1. Deveres e Responsabilidades da Contratante.

5.1.1. Designar formalmente, na forma do art. 177, da Lei nº 14.133/21, representantes para gerenciar e exercer a fiscalização da execução do Contrato, independentemente do acompanhamento e controle exercido pela Contratada.

5.1.2. Notificar a Contratada quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste TR, bem como quanto a qualquer ocorrência relativa ao comportamento de seus técnicos, quando em atendimento, que venha a ser

considerado prejudicial ou inconveniente para o Contratante.

5.1.3. Promover a fiscalização do contrato, sob os aspectos quantitativos e qualitativos, por intermédio de profissional especialmente designado, o qual anotará em registro próprio as falhas detectadas e as medidas corretivas necessárias. Ele deverá acompanhar o desenvolvimento do contrato, conferir os serviços executados e atestar os documentos fiscais pertinentes, quando comprovada a execução fiel e correta dos serviços, podendo, ainda, sustar, recusar, mandar fazer ou desfazer qualquer procedimento que não esteja de acordo com os termos avençados.

5.1.4. Proporcionar todas as facilidades indispensáveis ao bom cumprimento das obrigações avençadas, inclusive permitir acesso aos profissionais ou representantes da Contratada às suas dependências, quando necessário, e aos equipamentos e às soluções de software relacionados à execução do(s) serviço(s), mas com controle e supervisão das áreas técnicas.

5.1.5. Exigir o cumprimento de todos os compromissos assumidos pela Contratada, de acordo com os termos do contrato assinado.

5.1.6. Proporcionar todas as condições e prestar as informações necessárias para que a Contratada possa cumprir com suas obrigações, dentro das normas e condições contratuais.

5.1.7. Prestar, por meio do Fiscal Técnico do Contrato, as informações e os esclarecimentos pertinentes aos serviços/bens avençados, que porventura venham a ser solicitados pela Contratada.

5.1.8. Informar à Contratada sobre atos que possam interferir direta ou indiretamente nos serviços prestados/entrega de bens.

5.1.9. Comunicar oficialmente à Contratada, quaisquer falhas verificadas no cumprimento do contrato, determinando, de imediato, as providências necessárias à sua regularização.

5.1.10. Registrar e oficializar a Contratada sobre as ocorrências de desempenho ou comportamento insatisfatório, irregularidades, falhas, insuficiências, erros e omissões constatados, durante a execução do contrato, para as devidas providências.

5.1.11. Rejeitar, no todo ou em parte, os serviços executados que não atendam às especificações técnicas deste Termo de Referência.

5.1.12. Aprovar ou rejeitar, no todo ou em parte, os serviços executados ou entrega de equipamentos, que não estiverem em conformidade com as especificações constantes da proposta apresentada pela Contratada.

5.1.13. Efetuar o pagamento devido pela prestação dos serviços executados, desde que

cumpridas todas as formalidades e exigências avençadas.

5.1.14. Aplicar as sanções previstas em contrato, assegurando à Contratada o contraditório e a ampla defesa.

5.1.15. Exigir, sempre que necessário, a apresentação da documentação pela Contratada que comprove a manutenção das condições que ensejaram a sua contratação.

5.2. Deveres e Responsabilidades da Contratada

5.2.1. Manter atualizados seus dados cadastrais junto ao TJCE.

5.2.2. Responsabilizar-se pelo perfeito funcionamento do objeto da contratação. Isso significa que eventual omissão técnica constante neste documento deva ser suprida pela Contratada, sem ônus adicional ao TJCE.

5.2.3. Cumprir fielmente as especificações técnicas deste Termo de Referência.

5.2.4. Caberá a Contratada a responsabilidade pelo deslocamento, alimentação e estadia do seu técnico ao/no TJCE, quando estiver de maneira presencial realizando serviços, com todas as despesas de transporte, frete e seguro correspondentes.

5.2.5. Assumir total responsabilidade pela execução dos serviços, obedecendo ao que dispõe a proposta apresentada e observando as constantes do contrato e seus anexos, inclusive reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, vícios ou incorreções que forem detectados.

5.2.6. Ter pleno conhecimento de todas as condições e peculiaridades inerentes aos serviços objeto deste Termo de Referência, não podendo invocar, posteriormente, desconhecimento para cobrança de serviços extras.

5.2.7. Comunicar ao TJCE, por escrito, quaisquer anormalidades que ponham em risco o êxito e o cumprimento dos prazos da execução dos serviços, propondo as ações corretivas necessárias para a execução dos mesmos.

5.2.8. Submeter ao TJCE qualquer alteração que se tornar essencial à continuação da execução dos serviços.

5.2.9. Atender às solicitações emitidas pela Fiscalização quanto ao fornecimento de informações e/ou documentação.

5.2.10. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, o objeto do Contrato em que se verificarem vícios, defeitos ou incorreções que forem detectados durante a vigência do instrumento contratual, cuja responsabilidade lhe seja atribuível, exclusivamente.

5.2.11. Garantir a prestação dos serviços, mesmo em estado de greve da categoria, através de esquema de emergência.

5.2.12. Arcar com qualquer custo trabalhista em virtude da jornada de trabalho dos profissionais que vier a disponibilizar para a prestação de serviços.

5.2.13. Orientar seus empregados de que não poderão se retirar dos prédios ou instalações da Contratante portando volumes ou objetos sem a devida autorização e liberação do Fiscal do contrato.

5.2.14. Manter seus empregados identificados por crachá e uniformizados, quando nas dependências do Contratante, devendo substituir, no prazo estabelecido por ele, qualquer um deles que for inconveniente à boa ordem, demonstre incapacidade técnica, perturbe a ação da fiscalização, não acate as suas determinações ou não observe às normas internas.

5.2.15. Dar ciência aos empregados do conteúdo do contrato e das orientações contidas neste documento.

5.2.16. Responsabilizar-se por todas as providências e obrigações estabelecidas na legislação específica de acidentes do trabalho, quando, em ocorrência da espécie, forem vítimas os seus técnicos, na execução do serviço ou entrega de bens, ou em conexão com ele, ainda que acontecido em dependências do Contratante.

5.2.17. Arcar com o pagamento de eventuais multas aplicadas por quaisquer autoridades federais, estaduais e municipais/distrital, em consequência de fato a ela imputável e relacionado com o objeto do contrato.

5.2.18. Prever toda a mão-de-obra necessária para garantir a perfeita execução dos serviços ou entrega de bens, nos regimes contratados, obedecidas às disposições da legislação trabalhista vigente.

5.2.19. Responsabilizar-se pelo cumprimento das obrigações previstas em Acordo, Convenção, Dissídio, Coletivo de Trabalho ou equivalentes das categorias abrangidas pelo contrato, por todas as obrigações trabalhistas, sociais, previdenciárias, tributárias e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade à Contratante.

5.2.20. Promover a organização técnica e administrava dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram este Termo de Referência, no prazo determinado.

5.2.21. Manter, durante a vigência do Contrato, em compatibilidade com as obrigações assumidas, todas as condições de habilitação e qualificação apresentadas quando da assinatura do mesmo.

5.2.22. Comunicar ao Contratante, de imediato e por escrito, qualquer irregularidade verificada durante a execução do objeto, para a adoção das medidas necessárias à sua

regularização.

5.2.23. Não transferir a outrem, no todo ou em parte, a execução do contrato.

5.2.24. Responder civil e penalmente por quaisquer danos ocasionados à Administração e seu patrimônio e/ou a terceiros, dolosa ou culposamente, em razão de sua ação ou de omissão ou de quem em seu nome agir.

5.2.25. Responsabilizar-se pela conduta do empregado que for incompatível com as normas da Contratante, tais como: cometimento de ato desidioso, negligência, omissão, falta grave, violação do dever de fidelidade, indisciplina no descumprimento de ordens gerais e sigilo e segurança da informação.

5.2.26. Permitir a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo Contratante, em conformidade com o artigo 117 da Lei nº 14.133/21.

5.2.27. Aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessárias, nos termos do art. 125 da Lei 14.133/21.

5.2.28. Indenizar quaisquer danos ou prejuízos causados ao TJCE ou a terceiros, por ação ou omissão do seu pessoal durante a execução dos serviços/entrega de bens.

5.2.29. Não colocar à disposição da Contratante, para o exercício de funções de chefia, pessoal que incidam na vedação dos artigos 1º e 2º da Resolução nº 156/2012 do Conselho Nacional de Justiça (Art. 4º - Resolução 156/2012 – CNJ).

5.2.30. Encaminhar para o atesto dos fiscais, as faturas emitidas dos serviços prestados.

5.2.31. Guardar sigilo sobre dados e informações obtidos em razão da execução dos serviços ou entrega de bens, da relação contratual mantida com o Contratante.

5.2.32. Responsabilizar-se técnica e administrativamente pelo objeto do contrato, não sendo aceito, sob qualquer pretexto, a transferência de responsabilidade a outras entidades, sejam fabricantes, técnicos ou quaisquer outros.

5.2.33. Prestar os serviços contratados por meio de equipe técnica certificada na solução fornecida.

5.2.34. Não embaraçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Referência por servidor designado pelo Contratante.

5.2.34.1. A presença da fiscalização da Contratante não exime, de forma alguma, nem reduz a responsabilidade da Contratada.

5.2.35. Conceder acesso ao TJCE, o controle de atendimento para acompanhamento dos chamados técnicos, ficando o encerramento destes condicionados ao aceite do mesmo.

5.2.36. A Contratada deverá fornecer o licenciamento dos produtos, juntamente com as

chaves de ativação e todos os demais componentes necessários para a instalação e funcionamento impecável. Essa disponibilização deve abranger as versões especificadas no Edital, ou, quando aplicável, as versões mais recentes disponibilizadas pelo fabricante, de acordo com as especificações técnicas apresentadas em sua proposta comercial.

5.2.37. A Contratada deverá fornecer as credenciais de acesso ao site do fabricante. Isso permitirá a realização de downloads dos produtos adquiridos, bem como de correções, atualizações, drivers e quaisquer outros softwares de suporte disponibilizados. Deve ser mantida a conta corporativa em nome do TJCE, garantindo a continuidade desse acesso.

5.2.38. Caso não seja viável o download direto a partir do site do fabricante, a Contratada deverá fornecer mídias contendo os produtos objeto do contrato, sem qualquer custo adicional para o Contratante.

5.2.39. Contratada deve disponibilizar ao Contratante o acesso a Base de Conhecimento abrangente do fabricante, abordando informações sobre os produtos inclusos no contrato.

5.2.40. A Contratada deve fornecer um monitor de controle ou uma console de gerenciamento que abranja todas as licenças fornecidas e os direitos adquiridos, para o Contratante ter visibilidade e capacidade de gerenciar as licenças de forma eficaz.

5.2.41. A Contratada deve fornecer ao Contratante a documentação técnica completa e atualizada dos produtos adquiridos, incluindo manuais do fabricante, guias de instalação e quaisquer outros documentos pertinentes em suas versões originais.

5.3. Forma de Acompanhamento do Contrato

ID	Evento	Forma de Acompanhamento
1	Da entrega da solução	O recebimento do objeto deverá ocorrer conforme definido nos itens 3 e 4 e seus subitens.
2	Durante a vigência da garantia e suporte técnico.	Será verificado o cumprimento do prazo de solução dos chamados, conforme descrito no item 3.5 do documento.

5.4. Metodologia de Avaliação da Qualidade

5.4.1. Conforme item 3.

5.5. Níveis de Serviço

5.5.1. Conforme item 3.5.

5.6. Estimativa do Volume de Bens/Serviço

5.6.1. Conforme item 1.2.

5.7. Prazos e Condições

5.7.1. Os prazos são detalhados na seguinte Tabela:

N.º	Etapa	Quando	Responsável
1	Formalização da Ata de registro de Preços (ARP)	Após a homologação do certame.	Contratante
2	Assinatura do contrato	Após a emissão da Ordem de Fornecimento da ARP.	Contratante e Contratada
3	Reunião inicial	Em até 10 (dez) dias corridos contados após a assinatura do contrato.	Contratante e Contratada
4	Entrega das licenças conforme os requisitos apresentados no item 4.2.1 por parte da Contratada.	Em até 30 (trinta) dias corridos contados após o recebimento da ordem de serviço pela contratada.	Contratada
5	Implantação da solução conforme os requisitos apresentados no item 4.2.2 por parte da Contratada.	Em até 90 (noventa) dias corridos contados após o recebimento da ordem de serviço pela contratada.	Contratada
6	Treinamento da solução conforme os requisitos apresentados no item 4.2.3 por parte da Contratada.	Em até 90 (noventa) dias corridos contados após o recebimento da ordem de serviço pela contratada.	Contratada
7	Emissão do TRP da Contratante para a Contratada.	Após a validação e conclusão do fornecimento solicitado na ordem de serviço.	Contratante
8	Emissão do TRD da Contratante para a Contratada em caso de não possuir pendências ou solicitação de retificações para que a Contratada efetue as correções e solicite um novo TRP.	Em até 5 (cinco) dias úteis após a emissão do TRP.	Contratante
9	Início do período de validade/vigência dos serviços de suporte.	A partir da data de emissão do TRD.	Contratada

5.8. Do Reajuste

5.8.1. Conforme item 15.

5.9. Condições para Pagamento

5.9.1. Os pagamentos serão realizados através de depósito bancário, preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade, validado previamente pela Contratante atestada pelo setor competente deste Tribunal de Justiça, via emissão do Termo de Recebimento Definitivo, e também de apresentação de certidões que comprovem a regularidade da empresa com o fisco Federal, Estadual e Municipal, FGTS e INSS e débitos trabalhistas.

5.9.2. O prazo para pagamento de faturas ou notas fiscais serão suspensos durante o período de indisponibilidade do sistema de pagamento do Estado do Ceará ao final de cada exercício financeiro, aproximadamente entre 20 de dezembro e 31 de janeiro do ano subsequente, cujos pagamentos serão realizados até o final da primeira quinzena do mês de fevereiro.

5.9.3. O Tribunal de Justiça reserva-se ao direito de recusar o pagamento, no ato do atesto, caso o objeto não esteja em conformidade com as condições deste instrumento.

5.9.4. Nenhum pagamento será efetuado à empresa antes regularizada as sanções que por ventura lhe tenham sido aplicadas.

5.9.5. Nas notas fiscais referentes aos serviços objeto do contrato, deverão estar descriminados os valores dos tributos: impostos sobre serviços – ISS, PIS/PASEP, COFINS, FUST, FUNTTEL.

5.9.6. Constatada a situação de irregularidade da Contratada, será providenciada sua advertência, por escrito, para que, no prazo de 5 (cinco) dias, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do TJCE.

5.9.7. Não havendo regularização ou sendo a defesa considerada improcedente, o TJCE 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.

5.9.8. Persistindo a irregularidade, o TJCE deverá adotar as medidas necessárias a rescisão do contrato nos autos do processo administrativo correspondente, assegurada a

Contratada a ampla defesa.

5.9.9. 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

5.9.10. Somente por motivo de economicidade, segurança nacional ou outro interesse público de alta relevância, devidamente justificado, em qualquer caso, pela máxima autoridade do TJCE, não será rescindido o contrato em execução com a Contratada inadimplente.

5.9.11. Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) estar em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

5.9.12. O Tribunal de Justiça do Ceará não se responsabiliza por qualquer despesa bancária, nem por qualquer outro pagamento não previsto no instrumento contratual.

5.9.13. Havendo erro no documento de cobrança ou outra circunstância que desaprove a liquidação da despesa, a mesma ficará pendente e o pagamento sustado, até que a Contratada providencie as medidas saneadoras necessárias, não ocorrendo, neste caso, quaisquer ônus por parte do Contratante.

5.9.14. Os pagamentos efetuados à Contratada não a isentarão de suas obrigações e responsabilidades vinculadas ao fornecimento, especialmente aquelas relacionadas com a qualidade do produto.

5.9.15. A Contratada se obriga a manter as condições de habilitação e qualificação exigidas na contratação.

5.10. Propriedade, Sigilo, Restrições

5.10.1. A Contratada cederá ao Tribunal de Justiça do Estado do Ceará, nos termos do Art. 93, da LEI Nº 14.133, DE 1º DE ABRIL DE 2021, o direito patrimonial e a propriedade intelectual em caráter definitivo, os resultados produzidos em consequência do objeto contratado, entendendo-se por resultados quaisquer estudos, relatórios, artefatos, descrições técnicas, protótipos, dados, esquemas, plantas, desenhos, diagramas, roteiros, tutoriais, fontes dos códigos de programas computacionais em qualquer mídia, páginas de Intranet e Internet e qualquer outra documentação produzida no escopo da presenta contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros.

5.10.2. Toda a documentação produzida pela Contratada referente à implantação dos equipamentos e documentos exigidos no termo de referência passam a ser propriedade de forma perpétua do TJCE, não precisando este Tribunal de autorização

da Contratada para reproduzir, distribuir e publicar em documentos públicos ou fornecer a terceiros quando a administração considerar necessário.

5.10.3. Todas as informações obtidas ou extraídas pela Contratada quando da execução do objeto deverão ser tratadas como confidenciais, sendo vedada qualquer divulgação a terceiros, devendo a Contratada, zelar por si, por seus sócios, empregados e subcontratados (em outros contratos) pela manutenção do sigilo absoluto sobre os dados, informações, documentos, especificações técnicas e comerciais de que eventualmente tenham conhecimento ou acesso.

5.10.4. A obrigação assumida de Confidencialidade permanecerá válida durante o período de vigência do contrato principal e o seu descumprimento implicará em sanções administrativas e judiciais contra a Contratada, previstas no CONTRATO e na legislação pertinente.

5.10.5. Para efeito do cumprimento das condições de propriedade e confidencialidade estabelecidas, a Contratada exigirá de todos os seus empregados que, a qualquer título, venham a integrar a equipe executante do Objeto, a assinatura do Termo de Ciência, bem como a assinatura do Termo de Compromisso, onde o signatário e os funcionários que compõem seu quadro funcional declaram-se, sob as penas da lei, ciente das obrigações assumidas e solidário no fiel cumprimento das mesmas.

5.10.6. A Contratada deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de atualização, suporte e serviços especializados, manutenção e suporte, mediante assinatura do Termo de Confidencialidade.

5.11. Mecanismos Formais de Comunicação

Função de Comunicação	Emissor	Destinatário	Forma de Comunicação	Periodicidade
Emissão da Requisição de serviço/fornecimento	Contratante	Contratada	Requisição de serviço/fornecimento	Quando demandado pela SETIN.
Emissão da Nota de Empenho	Contratante	Contratada	Nota de empenho	Quando demandado pela SETIN.
Relato de alguma ocorrência contratual através de Ofício por	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a

correspondência.				algum item do contrato ou quando necessário.
Troca de informações técnicas necessárias a execução do contrato	Contratada/ Contratante	Contratante/ Contratada	Através de telefone, email, presencial, relatórios, documentos de texto, planilhas, slides, e-mail, sítios da internet, PDF (*Portable Document Format*): documento em formato portável.	Quando necessário

6. ESTIMATIVA DE PREÇO

6.1. Os valores de estimativa de custo total da contratação foram calculados com base nas médias identificadas no estudo de mercado da solução selecionada, considerando os valores unitários médios de cada componente.

6.2. Com base na demanda identificada, estima-se que será de 12.000 unidades de dispositivos a serem protegidos, sendo o quantitativo de 10.000 (dez mil) unidades de software EDR e 2.000 (dois mil) unidades de software XDR.

6.3. Além disso, será requerido o serviço de implantação e treinamento, conforme detalhado na tabela subsequente.

6.4. Os itens designados com ID 1 e 2, na tabela a seguir, podem ser contratados de maneira progressiva, para acomodar a variação natural do número de dispositivos utilizados.

Id	Objeto	Qtd de licenças	Vlr. Unit	Vlr. Total
1	Solução de Segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	10.000	**R$ 454,06**	**R$ 4.540.600,00**
2	Solução de Segurança de EndPoint XDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	2.000	**R$ 976,54**	**R$ 1.953.080,00**

3	Serviços de instalação, configuração e implantação da solução.	1	**R$ 137.030,26**	**R$ 137.030,26**
4	Treinamento.	1	**R$ 54.733,33**	**R$ 54.733,33**
Total				**R$ 6.685.443,59**

6.5. Na cotação de preços, é obrigatório abranger despesas relacionadas a impostos, taxas, frete, seguros e encargos sociais, trabalhistas, previdenciários, fiscais, comerciais e outros encargos de qualquer natureza que sejam necessários para a completa realização do objeto.

7. ADEQUAÇÃO ORÇAMENTÁRIA

Fonte	Fundo Especial de Modernização do Poder Judiciário do Ceará (FERMOJU)
Programa	192 - EXCELÊNCIA NO DESEMPENHO DA PRESTAÇÃO JURISDICIONAL
Ação	11470 - Desenvolvimento da Infraestrutura de TI (1° Grau) - FERMOJU 11473 - Desenvolvimento da Infraestrutura de TI (2° Grau) - FERMOJU
Natureza	INVESTIMENTO

ID	Serviço	Valor Unitário	Divisão	QTD Licenças	Valor Total
1	Solução de Segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	R$ 454,06	1° Grau	9.500	R$ 4.313.570,00
			2° Grau	500	R$ 227.030,00
2	Solução de Segurança de EndPoint XDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses.	R$ 976,54	1° Grau	1.900	R$ 1.855.426,00
			2° Grau	100	R$ 97.654,00

3	Serviços de instalação, configuração e implantação da solução.	R$ 137.030,26	1° Grau	1	R$ 137.030,26
4	Treinamento.	R$ 54.733,33	1° Grau	1	R$ 54.733,33
				VALOR GLOBAL	**R$ 6.685.443,59**

8. SANÇÕES APLICÁVEIS

8.1. Comete infração administrativa, nos termos da lei, a licitante que:

8.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pela Administração, em sede de diligência.

8.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

8.1.2.1. Não enviar a proposta ajustada após a negociação;

8.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

8.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva;

8.1.2.4. Deixar de apresentar amostra, quando exigível.

8.1.3. Não celebrar o contrato ou não entregar a garantia ou documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta.

8.1.4. Recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração.

8.1.5. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

8.1.6. Fraudar a licitação.

8.1.7. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

8.1.7.1. Agir em conluio ou em desconformidade com a lei;

8.1.7.2. Induzir deliberadamente a erro no julgamento;

8.1.7.3. Apresentar amostra falsificada ou deteriorada;

8.1.7.4. Praticar atos ilícitos com vistas a frustrar os objetivos da contratação;

8.1.7.5. Praticar ato lesivo previsto no art. 5° da Lei 12.846/2013.

8.2. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido no

instrumento convocatório, descrita no item 8.1.4, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação. A exigência da garantia obedecerá ao disposto no art. 58 da Lei nº 14.133/2021.

8.3. Com fulcro na Lei nº 14.133/2021, a Administração poderá, garantida a prévia defesa, aplicar a Contratada as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

8.3.1. Advertência;

8.3.2. Multa;

8.3.3. Impedimento de licitar e contratar; e

8.3.4. Declaração de inidoneidade para licitar ou contratar, enquanto perdurarem os motivos determinantes da punição ou até que seja promovida sua reabilitação perante a própria autoridade que aplicou a penalidade.

8.4. Na aplicação das sanções serão considerados:

8.4.1. A natureza e a gravidade da infração cometida;

8.4.2. As peculiaridades do caso concreto;

8.4.3. As circunstâncias agravantes ou atenuantes;

8.4.4. Os danos que dela provierem para a Administração Pública;

8.4.5. A implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.5. A sanção de multa calculada na forma do edital ou do contrato, não será inferior a 0,5% (cinco décimos por cento), nem superior a 30% (trinta por cento) do valor do contrato licitado ou celebrado com contratação, conforme §3º do art. 156 da Lei nº 14.133/2021.

8.5.1. A LICITANTE VENCEDORA, uma vez Contratada, sujeitar-se-á, em caso de inadimplemento de suas obrigações definidas neste Instrumento ou em outros que o complementem, às sanções e penalidades administrativas, inclusive multas.

8.5.1.1. Para as condutas descritas nos itens 8.1.5, 8.1.6 e 8.1.7, será aplicada multa de 30%.

8.5.1.2. Caso a Contratada não cumpra os prazos estabelecidos nos níveis de serviços, sem justificativa aceita, conforme descrito no item 3.5.19, estará sujeita a receber uma advertência. No caso de o atraso persistir por mais de 6 horas ou se houver reincidência, será aplicada uma multa no valor de 0,5%, acrescida de 0,1% por cada hora adicional de atraso.

8.5.1.3. No caso de atraso injustificado, nos prazos estabelecidos, na execução dos serviços constantes nos itens 4.2.1, 4.2.2 e 4.2.3, a Contratada ficará sujeita

a aplicação da multa, no valor de 0,5%, acrescida de 0,1% por dia de atraso.

8.5.1.3.1. Após o décimo dia de atraso injustificado, o Contratante poderá rescindir o contrato.

8.5.1.4. No caso de inexecução parcial do contrato ou descumprimento de obrigação contratual, será aplicada multa de 10% sobre o valor contratado.

8.5.1.5. No caso de inexecução total do contrato, será aplicada multa de 20% sobre o valor contratado.

8.5.2. A multa será recolhida no prazo máximo de 30 (trinta) dias úteis, a contar da comunicação oficial.

8.5.3. Os percentuais de multas aplicadas incidirão cumulativamente sempre sobre do valor global do termo de contrato licitado ou celebrado ou instrumento equivalente.

8.6. As sanções de advertência, impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar poderão ser aplicadas, cumulativamente ou não, à penalidade de multa.

8.7. Na aplicação da sanção será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação.

8.8. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 8.1.1, 8.1.2 e 8.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

8.9. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 8.1.4, 8.1.5, 8.1.6 e 8.1.7, bem como pelas infrações administrativas previstas nos itens 8.1.1, 8.1.2 e 8.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

8.10. A apuração de responsabilidade relacionadas às sanções de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar demandará a instauração de processo de responsabilização a ser conduzido por comissão composta por 2 (dois) ou mais servidores estáveis, que avaliará fatos e circunstâncias conhecidos e intimará o licitante ou o adjudicatário para, no prazo de 15 (quinze) dias úteis, contado da data de sua intimação, apresentar defesa escrita e especificar as

provas que pretenda produzir.

8.11. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

8.12. Caberá a apresentação de pedido de reconsideração da aplicação da sanção de declaração de inidoneidade para licitar ou contratar no prazo de 15 (quinze) dias úteis, contado da data da intimação, e decidido no prazo máximo de 20 (vinte) dias úteis, contado do seu recebimento.

8.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

8.14. A aplicação das sanções previstas neste edital não exclui, em hipótese alguma, a obrigação de reparação integral dos danos causados.

8.15. Sempre que houver irregularidade na prestação dos serviços executados, o TJCE efetuará a apuração das ocorrências e comunicará à Contratada, conforme especificado.

8.16. As notificações de multas e sanções são de responsabilidades da Coordenadoria Central de Contratos e Convênios do TJCE, que receberá da unidade administrativa responsável e gestora do contrato os relatórios com as ocorrências insatisfatórias que comprometam a execução do termo de contrato.

8.17. Nenhuma sanção será aplicada sem o devido processo administrativo, oportunizando-se defesa prévia ao interessado e recurso nos prazos definidos em lei, sendo-lhe franqueada vistas ao processo.

9. CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. Proposta de Preço

9.1.1. A proposta deverá conter obrigatoriamente os seguintes elementos:

9.1.1.1. Preço unitário por item, em moeda corrente nacional, cotados com apenas duas casas decimais, expressos em algarismos e por extenso, sendo que, em caso de divergência entre os preços expressos em algarismos e por extenso, serão levados em consideração os últimos;

9.1.1.2. Não deve conter cotações alternativas, emendas, rasuras ou entrelinhas;

9.1.1.3. Deve fazer menção ao número do pregão e do processo licitatório;

9.1.1.4. Deve ser datada e assinada na última folha e rubricadas nas demais, pelo representante legal da empresa;

9.1.1.5. Deve conter na última folha o número do CNPJ da empresa;

9.1.1.6. Deve informar o prazo de validade da proposta, que não poderá ser inferior a 60 (sessenta) dias corridos, contados da data de entrega da mesma;

9.1.1.7. Deverá conter a descrição detalhada do objeto, tais como: somente uma única marca, modelo, características do objeto, procedência e demais dados que a licitante julgar necessário;

9.1.1.8. Indicação do nome do banco, número da agência, número da conta corrente, para fins de recebimento dos pagamentos.

9.1.1.9. Deverá ser anexado junto a sua proposta, documento contendo o item do Edital e sua referência comprobatória, informando/indicando/referenciando as referidas documentações técnicas comprobatórias.

9.2. Modalidade e Tipo de Licitação

9.2.1. A modalidade da licitação sugerida é o pregão eletrônico para registro de preços, em conformidade com a Lei 14.133/21, tendo em vista o objeto se tratar de bem e serviço comum, cujos padrões de qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado, para o fornecimento de licença de software e prestação de serviços de implantação e treinamento.

9.2.2. A licitação será do tipo menor preço. Os valores máximos aceitáveis, tanto unitários quanto global, estão descritos no item 6.

9.3. Justificativa de Adoção da Modalidade da Licitação

9.3.1. Modalidade de Licitação

9.3.1.1. A aquisição da solução em questão é comum no mercado, uma vez que possui características padronizadas e amplamente utilizadas. Dessa forma, é fácil encontrar empresas que ofereçam serviços de fornecimento, manutenção, suporte e garantia para essa solução. Devido à alta demanda por esses serviços tanto no setor privado quanto no público, há uma ampla gama de fornecedores disponíveis, com diferentes níveis de expertise e qualidade.

9.3.1.2. Diante desse cenário, optou-se por realizar uma licitação para registro de preços via Pregão, na modalidade eletrônica, utilizando o critério de menor preço individual, previamente ao menor preço individual de cada item, e adotando um modo de disputa aberto e fechado. Isso permite uma maior competitividade no certame, garantindo que as empresas concorram em condições equitativas.

9.3.1.3. Nos critérios de habilitação técnica, não será exigido prazo de validade dos atestados de capacidade técnica. Essa decisão busca promover uma maior competitividade no processo licitatório, sem, no entanto, ferir os princípios legais. Vale ressaltar que o objeto a ser licitado é comum no mercado e não requer uma existência muito longa, o que justifica a não imposição de limites de tempo para os atestados de capacidade técnica.

9.4. Qualificação Econômico-Financeira

9.4.1. A Qualificação Econômico-Financeira tem como objetivo avaliar a capacidade financeira e econômica das empresas interessadas em participar da concorrência, garantindo assim a segurança do contrato e a viabilidade do projeto. No Tribunal de Justiça do Ceará, a Qualificação Econômico-Financeira é um critério importante para a escolha da empresa vencedora, pois garante a solvência financeira e a capacidade de cumprimento do contrato firmado.

9.4.2. Certidão negativa de falência, concordata, recuperação judicial ou extrajudicial, expedida por quem de competência na sede da pessoa jurídica ou certidão negativa de execução patrimonial expedida no domicílio da pessoa física.

9.4.3. No caso de cooperativa, a mesma está dispensada da apresentação da Certidão exigida no subitem acima.

9.4.4. **BALANÇO PATRIMONIAL** e demonstrações contábeis do último exercício social, já exigíveis e apresentados na forma da lei, que comprovem a boa situação financeira do licitante, vedada a sua substituição por balancetes ou balanços provisórios, podendo ser atualizados por índices oficiais, quando encerrado há mais de 03 meses da data de apresentação da proposta.

9.4.5. **COMPROVAÇÃO DA BOA SITUAÇÃO FINANCEIRA** atestada por documento, assinado por profissional legalmente habilitado junto ao Conselho Regional de Contabilidade da sede ou filial do licitante, demonstrando que a empresa apresenta índice de Liquidez Geral (LG) maior ou igual a 1,0 (uma vírgula zero), calculada conforme a fórmula abaixo:

$$\mathbf{LG = (AC + ARLP)/(PC + PELP) \geq 1,0}$$

Onde:

LG – Liquidez Geral.

AC – Ativo Circulante.

ARLP – Ativo Realizável a Longo Prazo.

PC – Passivo Circulante.

PELP – Passivo Exigível a Longo Prazo.

9.4.6. No caso de sociedade por ações, o balanço deverá ser acompanhado da publicação em jornal oficial, em jornal de grande circulação e do registro na Junta Comercial.

9.4.7. No caso das demais sociedades empresárias, o balanço deverá ser acompanhado dos termos de abertura e de encerramento do Livro Diário - estes termos devidamente registrados na Junta Comercial - constando ainda, no balanço, o número do Livro Diário e das folhas nos quais se acha transcrito ou autenticada na junta comercial, devendo tanto o balanço quanto os termos ser assinados por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

9.4.8. No caso de empresa recém-constituída (há menos de 01 ano), deverá ser apresentado o balanço de abertura acompanhado dos termos de abertura e de encerramento devidamente registrados na Junta Comercial, constando no balanço o número do Livro e das folhas nos quais se acha transcrito ou autenticado na junta comercial, devendo ser assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da empresa.

9.4.9. No caso de sociedade simples e cooperativa - o balanço patrimonial deverá ser inscrito no Cartório de Registro Civil de Pessoas Jurídicas assinado por contador registrado no Conselho Regional de Contabilidade e pelo titular ou representante legal da instituição, atendendo aos índices estabelecidos neste instrumento convocatório.

9.4.10. **PATRIMÔNIO LÍQUIDO MÍNIMO** não inferior a 10% da estimativa de custos, que deverá ser comprovado através da apresentação do balanço patrimonial.

9.4.11. A comprovação solicitada visa garantir que a Contratada possua capacidade e porte suficiente para atender ao objeto desta contratação, bem como a capacidade financeira de sustentar suas atividades diante das oscilações de demandas que ocorrem durante a vigência do contrato.

9.5. Qualificação Técnica

9.5.1. Com o intuito de minimizar os riscos da contratação e alcançar os resultados esperados, é imprescindível que o LICITANTE possua capacidade técnica e de

fornecimento para executar o objeto da licitação.

9.5.2. A exigência de comprovação de capacidade técnica relacionada ao objeto licitado se dá com fulcro no Art. 67 inciso I da Lei nº 14.133/21 e visa garantir que a LICITANTE já forneceu os serviços a serem contratados e, portanto, possui capacidade técnico-operacional para fornecê-lo adequadamente.

9.5.3. A LICITANTE deve apresentar o Atestado de Capacidade Técnica, emitido por pessoa jurídica de direito público ou privado, atestando que a licitante já forneceu, de maneira satisfatória, produtos similares em termos de quantidade e características ao objeto da presente licitação.

9.5.3.1. Em relação à especificação, considera-se compatível, serviço de implantação de solução de antivírus (software) com EDR ou XDR, não sendo necessário que corresponda exatamente às especificações detalhadas no item 3.4 deste Termo de Referência (TR).

9.5.3.2. No que se refere ao quantitativo, será considerado compatível o fornecimento de, no mínimo, 5% (cinco por cento) do total previsto cumulativamente para as soluções identificadas como 1 e 2 no Item 1.2 deste TR.

9.5.3.2.1. Para comprovar o quantitativo, será aceito o somatório dos atestados apresentados.

9.5.4. O TJCE reserva o direito de conduzir diligências junto aos fabricantes para verificar o cumprimento das exigências de comercialização destinadas à Administração Pública.

9.5.5. A LICITANTE disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados.

9.5.6. Caso a LICITANTE não comprove as exigências previstas neste Termo de Referência por meio das documentações requeridas, será desclassificada.

9.5.7. O atestado deverá conter:

9.5.7.1. Razão Social, CNPJ e Endereço Completo da Empresa ou Órgão Emitente.

9.5.7.2. Razão Social da Contratada.

9.5.7.3. Número e vigência do contrato.

9.5.7.4. Objeto do contrato.

9.5.7.5. Local e Data de Emissão.

9.5.7.6. Assinatura do responsável pela emissão do atestado.

9.5.8. Tratando-se de empresa ou sociedade estrangeira em funcionamento no país, deve possuir Decreto de Autorização e Ato de Registro, ou autorização para

funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

9.5.9. A não comprovação de alguma característica exigida, quando solicitada pelo Contratante, levará à desclassificação da proposta.

9.5.10. No caso de atestados emitidos por empresa da iniciativa privada, não serão considerados válidos aqueles emitidos por empresas pertencentes ao mesmo grupo empresarial da LICITANTE. Serão considerados como pertencentes ao mesmo grupo empresarial da empresa proponente, empresas controladas ou controladoras da empresa proponente, ou que tenha pelo menos uma mesma pessoa física ou jurídica que seja sócio da empresa emitente e da empresa proponente.

9.5.11. O TJCE reserva-se o direito de realizar diligências, a qualquer momento, com o objetivo de verificar se o(s) atestado(s) e demais documentos são adequados e atendem às exigências contidas no Termo de Referência, podendo buscar por meios próprios ou exigir a apresentação de documentação complementar, tais como Notas Fiscais, Contratos, Atas do Pregão Original, entre outros, referente à prestação de serviços relativos aos atestados apresentados

9.5.12. É permitido o agrupamento de atestados de capacidade técnico-operacional, a fim de comprovar a experiência na prestação de serviços com características técnicas semelhantes ao objeto desta contratação.

9.5.13. A comprovação de capacidade técnica estará sujeita à confirmação da veracidade de suas informações através de possíveis diligências, conforme prescreve o art. 59, § 2º, da Lei 14.133/21.

9.5.14. Por fim, caso a empresa esteja sob falência, concurso de credores, dissolução ou liquidação, deve apresentar Plano de Recuperação Judicial, devidamente homologado. Se nessas condições e, ainda, sendo formada em consórcio de empresas, esta não deverá ser controladora, coligada ou subsidiária entre si, devendo, da mesma forma, apresentar Plano de Recuperação Judicial, devidamente homologado.

10. GARANTIA CONTRATUAL

10.1. A Contratada deverá entregar ao Gerente de Contratação do objeto, que submeterá à Coordenadoria Central de Contratos e Convênios do TJCE, no prazo prescrito no art. 96 da Lei n.º 14.133/2021, a título de garantia, a quantia equivalente a 5% (cinco por cento) do valor global da contratação, cabendo-lhe optar dentre as modalidades previstas no art. 96, Lei n.º 14.133/2021.

10.1.1. A garantia será devolvida à Contratada somente depois do cumprimento integral das

obrigações assumidas, inclusive recolhimento de multas e satisfação de prejuízos causados ao Contratante.

10.1.2. Será exigida do licitante vencedor a indicação na sua proposta a modalidade da garantia escolhida, a fim de possibilitar a contagem do prazo de acordo com cada modalidade.

10.2. A garantia, qualquer que seja a modalidade escolhida, assegurará o pagamento de:

10.2.1. Prejuízo advindo do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas.

10.2.2. As multas moratórias e punitivas aplicadas pelo Contratante à Contratada.

10.2.3. Obrigações trabalhistas e previdenciárias de qualquer natureza, não adimplidas pela Contratada, quando couber.

10.3. A Contratada terá o prazo mínimo de 1 (um) mês, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pela modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

10.3.1. A apólice deverá seguir as regras estatuídas na Circular Susep nº 662, de 11 de abril de 2022, quando da escolha por parte do licitante vencedor da modalidade prevista no inciso II do § 1º artigo 96 da Lei Nº 14.133/21.

10.3.2. O seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas, conforme inciso II do artigo 97 da Lei Nº 14.133/21.

10.3.3. A modalidade seguro-garantia somente será aceita se contemplar todos os eventos indicados neste documento, observada a legislação que rege a matéria.

10.4. A Contratada terá o prazo mínimo de 10 (dez) dias corridos, contando do recebimento do termo de intenção de contratação e anterior à assinatura do contrato, para a prestação da garantia quando esta optar pelas demais modalidades previstas no § 1º do art. 96, da Lei Nº 14.133/21.

10.4.1. A garantia em dinheiro deverá ser efetuada em instituição bancária indicada pelo Contratante, com correção monetária, em favor do Contratante.

10.4.2. Caso a opção seja por utilizar títulos da dívida pública, estes devem ter sido emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados pelos seus valores econômicos, conforme definido pelo Ministério da Fazenda.

10.4.3. No caso de garantia na modalidade de fiança bancária, deverá constar expressa renúncia do fiador aos benefícios do artigo 827 do Código Civil.

10.5. A garantia deverá ter validade durante a execução do contrato de 90 (noventa) dias após término da vigência contratual, devendo acompanhar as modificações referentes ao valor e à vigência desta mediante a complementação da caução ou emissão do respectivo endosso pela seguradora ou instituição bancária fiadora.

10.5.1. O prazo para complementação da caução ou emissão do endosso da garantia referente aos aditivos contratuais deverá seguir os mesmos prazos estabelecidos nos subitens 10.3 e 10.4.

10.6. Caso o valor da garantia seja utilizado no todo ou em parte para o pagamento de multas, ela deve ser complementada no prazo de até 10 (dez) dias úteis, contados da solicitação do Contratante, a partir do qual se observará o disposto abaixo:

10.6.1. A não complementação ou renovação, tempestiva, da garantia do contrato ensejará a suspensão de pagamentos até a regularização do respectivo documento, independentemente da aplicação das sanções contratuais.

10.6.2. A inobservância do prazo fixado para apresentação, complementação ou renovação da garantia acarretará a aplicação das sanções previstas neste Termo de Referência.

10.7. O garantidor não é parte interessada para figurar em processo administrativo instaurado pelo Contratante com o objetivo de apurar prejuízos e/ou aplicar sanções à Contratada.

10.8. A garantia será considerada extinta:

10.8.1. Com a devolução da apólice, carta fiança ou autorização para o levantamento de importâncias depositadas em dinheiro ou títulos da dívida pública, acompanhada de declaração do Contratante, mediante termo circunstanciado, de que a Contratada cumpriu todas as cláusulas do contrato.

10.8.2. No prazo de 90 (noventa) após o término da vigência, caso o Contratante não comunique a ocorrência de sinistros.

10.9. A ausência de prestação da garantia equivale à recusa injustificada para a contratação, caracterizando descumprimento total da obrigação assumida, ficando a adjudicatária sujeita às penalidades legalmente estabelecidas, inclusive multa e rescisão unilateral do contrato administrativo.

11. ÓRGÃO GESTOR GERAL DE REGISTRO DE PREÇOS E PARTICIPANTE DO REGISTRO DE PREÇOS

11.1. O Tribunal de Justiça do Estado do Ceará será o órgão gestor geral e único participante no presente registro de preços.

11.2. A Intenção de Registro de Preços (IRP) é a ferramenta que permite que Administração

Pública compartilhe as suas intenções de realizar licitações para Registro de Preço - SRP, possibilitando a participação de outros órgãos ou entidades que tenham interesse em adquirir o mesmo objeto, possibilitando auferir melhores preços por meio de economia de escala.

11.3. Quanto à divulgação da IRP, registra-se que o art. 86 da Lei nº 14.133/2021, dispõe de tal exigência, como se observa a partir da leitura do seguinte dispositivo legal:

11.3.1. "Art. 86. O órgão ou entidade gerenciadora deverá, na fase preparatória do processo licitatório, para fins de registro de preços, realizar procedimento público de intenção de registro de preços para, nos termos de regulamento, possibilitar, pelo prazo mínimo de 8 (oito) dias úteis, a participação de outros órgãos ou entidades na respectiva ata e determinar a estimativa total de quantidades da contratação."

11.4. Assim, vislumbra-se que, embora seja regra a divulgação da Intenção de Registro de Preços pelos órgãos, em razão da finalidade de tal procedimento, é perfeitamente cabível o seu afastamento, desde que haja justificativa adequada, conforme art. 86, § 1º, a seguir transcrito:

11.4.1. Art 86 "§ 1º O procedimento previsto no caput deste artigo será dispensável quando o órgão ou entidade gerenciadora for o único contratante."

11.5. Dessa forma, o Tribunal de Justiça do Estado do Ceará, optou pela não divulgação da referida Intenção de Registro de Preços (IRP), conforme observações abaixo:

11.5.1. Ausência de estrutura administrativa satisfatória para fins de gerenciamento das Atas de Registro de Preços.

11.5.2. Ausência de recursos humanos, tendo em vista, que possuímos um grande volume de processos licitatórios, atas de registro de preços e contratos a serem geridos anualmente, o que por si só exige extrema dedicação, concentração, celeridade e manutenção aceitável de qualidade no gerenciamento das contratações da Secretaria de Tecnologia da Informação.

12. DO ÓRGÃO GERENCIADOR DA ATA DE REGISTRO DE PREÇOS

12.1. A Ata de Registro de Preços será gerida pela Secretaria de Tecnologia da Informação, podendo ser nomeado um servidor específico para fiscalizar a execução do objeto registrado e as condições de habilitação do fornecedor.

13. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

13.1. Não será permitida adesão à Ata de Registro de Preço decorrente deste Pregão.

14. DA ASSINATURA DA ATA E DA CONTRATAÇÃO COM FORNECEDORES REGISTRADOS

14.1. O fornecedor adjudicatário será convocado para assinar a ata de registro de preços, no prazo de até 5 (cinco) dias úteis após a homologação da licitação ou contratação direta, a contar da data do recebimento da convocação, nas condições estabelecidos no instrumento convocatório, podendo o prazo ser prorrogado por uma vez, por igual período, quando solicitado e desde que ocorra motivo justificado, aceito pela administração.

14.1.1. Serão incluídos na ata de registro de preços, na forma de anexo, os licitantes que aceitaram integrar o cadastro de reserva e os demais classificados da licitação.

14.1.2. A recusa do fornecedor adjudicatário em assinar a ata de registro de preços caracteriza o descumprimento total das obrigações assumidas, sujeitando-o às penalidades.

14.1.3. É facultado à Administração, obedecendo a ordem de classificação, convocar os licitantes do cadastro de reserva ou, se não houver, os remanescentes da licitação para assinarem a ata de registro de preços, em igual prazo e nas mesmas condições propostas pelo vencedor, quando este não atender a convocação prevista neste subitem ou no caso da exclusão do detentor do preço registrado, nas hipóteses previstas no item 16.

14.1.4. O licitante convocado nos termos do subitem 14.1.3 deverá comprovar as condições de habilitação exigidas no certame e apresentar proposta compatível com o objeto pretendido pela Administração.

14.1.5. No caso do licitante convocado não atender as exigências previstas no subitem 14.1.4, a Administração convocará os demais licitantes do cadastro de reserva ou, se não houver, os remanescentes da licitação, obedecendo a ordem de classificação do certame.

14.1.6. Na hipótese de nenhum dos licitantes aceitarem assinar a ata de registro de preços nos termos do disposto no subitem 14.1.3, a Administração poderá convocar os licitantes remanescentes, obedecendo a ordem de classificação, para a assinatura da ata nas condições ofertadas por estes, desde que o preço seja igual ou inferior, ou o percentual de desconto igual ou superior, ao estimado para a contratação, nos termos do instrumento convocatório.

14.1.7. A ata de registro de preços poderá, a critério da Administração, ser assinada por certificação digital.

14.2. As contratações serão formalizadas por meio de contrato administrativo, ordem de compra ou de serviço, nota de empenho ou outro instrumento hábil, conforme o disposto no artigo 95 da Lei nº 14.133, de 01 de abril de 2021.

14.2.1. Quando o contratante for empresa pública, sociedade de economia mista ou suas subsidiárias, a formalização, a que se refere o subitem 14.2, deverá observar o disposto na

seção I do capítulo II da Lei Federal nº 13.303, de 30 de junho de 2016.

14.2.2. São competentes para realizar as contratações os titulares dos órgãos e entidades participantes da ata de registro de preços e o representante do fornecedor detentor do preço registrado ou seu procurador legalmente habilitado.

14.3. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente motivada.

14.3.1. O fornecedor detentor de preço registrado não está impedido de participar de outros processos para contratação do mesmo objeto.

15. DA REVISÃO DOS PREÇOS REGISTRADOS

15.1. Os preços registrados serão fixos e irreajustáveis durante a vigência da ata, exceto em decorrência das disposições contidas na alínea d, do inciso II, do artigo 124 e no artigo 134 da Lei nº 14.133, de 01 de abril de 2021;

15.2. O órgão ou entidade gerenciadora ao constatar a existência de preço registrado acima dos preços de mercado, deverá:

15.2.1. Convocar o fornecedor do preço registrado para o bem ou serviço, visando a negociação para a redução de preços e sua adequação ao mercado;

15.2.2. Liberar o fornecedor do compromisso assumido, sem aplicação de penalidade, e cancelar o preço registrado objeto da negociação, quando essa for frustrada, respeitadas as contratações realizadas;

15.2.3. Convocar os demais fornecedores do cadastro de reserva ou, se não houver, os remanescentes que atenderem os termos do disposto nos subitens 14.1.3, 14.1.5 e 14.1.6, pela ordem, para assegurar igual oportunidade de negociação.

15.3. O fornecedor detentor do registro de preço ao constatar preços de mercado superiores ao registrado, observado o disposto no caput deste artigo, poderá requerer o reequilíbrio de preço, mediante justificativa e comprovação, ao órgão ou entidade gerenciadora, que poderá:

15.3.1. Rever o preço registrado, cuja aplicação somente ocorrerá nas contratações posteriores ao recebimento do requerimento;

15.3.2. Indeferir, por interesse da Administração, o requerimento, e liberar o fornecedor do compromisso assumido, sem aplicação de penalidade, desde que confirmada a veracidade dos motivos e dos documentos apresentados, e que o requerimento ocorra antes do recebimento da ordem de compra ou de serviço;

15.3.3. Convocar os demais fornecedores do cadastro de reserva ou, se não houver, os

remanescentes que atenderem os termos do disposto nos subitens 14.1.3, 14.1.5 e 14.1.6, pela ordem, para assegurar igual oportunidade de negociação.

15.4. O requerimento a que se refere o subitem 15.3 somente será admitido após 90 (noventa) dias da data de publicação da ata de registro de preços, salvo nos casos de tributos ou encargos legais criados, alterados ou extintos, bem como a superveniência de disposições legais, quando ocorridas após a data da apresentação da proposta, de comprovada repercussão nos preços contratados.

15.5. Não havendo êxito nas negociações, o órgão ou entidade gerenciadora cancelará o bem ou serviço registrado e comunicará aos órgãos ou entidades participantes.

15.6. Caso haja alteração do preço registrado, o órgão ou entidade gerenciadora comunicará o fato aos órgãos ou entidades participantes.

15.7. A alteração do preço registrado não altera automaticamente o preço do contrato decorrente da ata de registro de preços, cuja revisão deverá ser feita pelo órgão ou entidade contratante, observadas as disposições legais incidentes sobre os contratos.

16. DO CANCELAMENTO DO REGISTRO DE PREÇOS

16.1. O fornecedor detentor de preço registrado em ata terá os seus bens, obras ou serviços cancelados nas seguintes hipóteses:

16.1.1. Descumprir as condições da ata de registro de preços;

16.1.2. Não confirmar o recebimento da ordem de compra ou serviço, da nota de empenho ou de outro instrumento hábil ou recusar-se a realizar as contratações decorrentes do registro de preços, total ou parcialmente, no prazo estabelecido pela Administração, sem justificativa aceitável;

16.1.3. Não aceitar reduzir o seu preço registrado, na hipótese deste se tornar superior aos praticados no mercado, conforme disposto no subitem 15;

16.1.4. For liberado do compromisso, nos termos do subitem 15;

16.1.5. Sofrer sanção prevista nos termos do artigo 156, incisos III e IV, da Lei Federal nº 14.133, de 01 de abril de 2021, ou do artigo 83, inciso III, da Lei Federal nº 13.303, de 30 junho de 2016;

16.1.6. For por razões de interesse público, devidamente fundamentadas;

16.1.7. For amigável, nos termos do artigo 138, inciso II, da Lei Federal nº 14.133, de 01 de abril de 2021;

16.1.8. For por ordem judicial;

16.1.9. Por solicitação do próprio fornecedor, em caso fortuito ou força maior, que comprometa a execução ou o fornecimento, devidamente comprovado e justificado.

17. DA ASSINATURA DO CONTRATO

17.1. A empresa fornecedora da Ata de Registro de Preços deverá assinar o Contrato dentro do prazo de 5(cinco) dias úteis, contados a partir da sua convocação.

17.2. O prazo estabelecido no subitem anterior poderá ser prorrogado uma vez, por igual período, quando solicitado pelo fornecedor e desde que ocorra motivo justificado aceito pela Administração.

17.3. A recusa injustificada do licitante vencedor ou dos classificados no cadastro reserva em assinar a ata, dentro do prazo estabelecido no subitem 17.1, ensejará a aplicação das penalidades previstas no instrumento convocatório.

18. VIGÊNCIA DA ATA DE REGISTRO DE PREÇOS

18.1. O prazo de vigência da ata de registro de preços será de 1 (um) ano, contado a partir da data da sua publicação no Diário da Justiça Eletrônico, e poderá ser prorrogado, por igual período, desde que por acordo entre as partes e comprovado o preço vantajoso, nas mesmas condições e quantidades ou valores remanescentes.

19. VIGÊNCIA CONTRATUAL

19.1. A vigência do contrato terá início na data de sua assinatura e se estenderá por um período de até 12 (doze) meses.

Equipe de Planejamento da Contratação

Diego Francisco de Mesquita Oliveira - 48802

Integrante Técnico

Francisco José Pessoa Furtado – 8284

Integrante Administrativo

Cristiano Henrique Lima de Carvalho – 5198

Área Demandante

Heldir Sampaio Silva - 9630

Integrante Demandante

20. APROVAÇÕES

Aprovo. Encaminha-se para iniciação de procedimento licitatório.

Autoridade Competente

Denise Maria Norões Olsen – 24667

Fortaleza, 17 de maio de 2024.