

**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 E DEMAIS ESPECIFICAÇÕES E CARACTERÍSTICAS CONSIGNADOS, INCLUINDO SUPORTE E GARANTIA PELO PERÍODO DE 60 MESES, SOB REGIME DE EMPREITADA POR PREÇO UNITÁRIO, QUE ENTRE SI CELEBRAM O TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ E A EMPRESA NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA. (PROCESSO ADMINISTRATIVO N. 8510187-89.2024.8.06.0000).**

**CT N.º 63/2024**

**CÓDIGO DA CONTRATAÇÃO (PAC): TJCESETIN\_2024\_0011**

O **TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ**, situado no Centro Administrativo Governador Virgílio Távora, com sede na Avenida General Afonso Albuquerque Lima, S/N, Bairro Cambeba, Fortaleza – CE, inscrito no CNPJ sob o número 09.444.530/0001-01, doravante denominado simplesmente de TJCE ou CONTRATANTE, neste ato representado por seu Presidente, Des. Antônio Abelardo Benevides Moraes e por sua Secretária de Tecnologia da Informação, Denise Maria Norões Olsen, e a empresa **NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA.**, representada neste ato por Yure Leopoldo Sabino de Freitas, portador da carteira de identidade n. 559056187 SSP/SP, CPF n. 525.285.023-20, com endereço na Av. Dom Manuel, 1020 - Sala 02 - Bairro Centro, em Fortaleza/CE, inscrita no CNPJ sob o número 05.250.796/0001-54, daqui por diante simplesmente denominada CONTRATADA, pactuam o presente Contrato, que se regerá pela Lei n. 14.133, de 21 de abril de 2021 e pela Resolução n. 169, de 31 de janeiro de 2013, do Conselho Nacional de Justiça, com suas alterações e atualizações posteriores.

#### **CLÁUSULA PRIMEIRA – DA FUNDAMENTAÇÃO LEGAL**

Fundamenta-se o presente Instrumento na proposta apresentada pela CONTRATADA e no resultado da licitação realizada sob a modalidade Pregão Eletrônico n. 28/2024, devidamente homologada pelo Exmo. Desembargador Presidente do Tribunal de Justiça do Estado do Ceará, tudo em conformidade com as disposições da Lei Nacional n. 14.133/2021, com suas alterações e atualizações posteriores, e o processo administrativo n. 8510187-89.2024.8.06.0000.

#### **PARÁGRAFO ÚNICO – REGIME DE CONTRATAÇÃO**

A execução da presente avença será indireta, segundo o regime de execução por preço unitário, nos termos dos art. 6º, XXVIII da Lei n. 14.133/21, sendo originário da licitação na modalidade de Pregão, na forma eletrônica, sob o número 28/2024.

## **CLÁUSULA SEGUNDA – DO OBJETO**

O objeto deste Instrumento consiste na *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 e demais especificações e características consignados, incluindo suporte e garantia pelo período de 60 meses*, sob regime de execução indireta, conforme especificações contidas no Edital do Pregão Eletrônico n. 24/2024 e seus anexos, bem como nos Anexos deste Contrato, todos, partes do mesmo.

### **§ 1º DOCUMENTAÇÃO COMPLEMENTAR**

Os documentos constantes do Processo Administrativo nº. 8510187-89.2024.8.06.0000 integram o presente Termo de Contrato como se nele estivessem transcritos, cujos teores consideram-se conhecidos e acatados pelas partes, sem prejuízos da aplicação de normas técnicas e legislação vigentes relativas ao objeto contratual, especialmente quanto a(ao):

- a. Termo de Referência;
- b. Edital e demais anexos do Edital de Pregão Eletrônico nº 28/2024; e,
- c. Proposta da CONTRATADA, no que couber.

§ 2º A prestação dos serviços obedecerá ao estipulado neste Contrato, bem como às disposições assumidas na proposta firmada pela CONTRATADA, dirigida ao CONTRATANTE, independentemente da transcrição, a qual faz parte integrante e complementar deste Contrato, no que não o contrarie.

## **CLÁUSULA TERCEIRA – DAS OBRIGAÇÕES DAS PARTES**

São obrigações das partes neste Termo de Contrato:

### **§ 1º DO CONTRATANTE**

I. 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.

II. Notificar a CONTRATADA quanto a irregularidades ou defeitos verificados na execução das atividades objeto deste contrato, 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.

III. 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.

IV. 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.

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

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

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

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

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

X. 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.

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

XII. 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.

XIII. Efetuar o pagamento devido pela prestação dos serviços executados, desde que cumpridas todas as formalidades e exigências avançadas.

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

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

## **§ 2º DA CONTRATADA**

I. Manter atualizados seus dados cadastrais junto ao TJCE.

II. 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.

III. Cumprir fielmente os Instrumentos as especificações técnicas do Anexo I do Edital.

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

V. 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.

VI. 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.

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

VIII. 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.

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

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

XI. 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.

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

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

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

XV. 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.

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

XVII. 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.

XVIII. 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.

XIX. 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.

XX. 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.

XXI. Promover a organização técnica e administrativa dos serviços, de modo a conduzi-los eficaz e eficientemente, de acordo com os documentos e especificações que integram o ANEXO I do Edital, no prazo determinado.

XXII. 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.

XXIII. 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.

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

XXV. 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.

XXVI. Responsabilizar-se pela conduta do empregado que for incompatível com as normas do 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.

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

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

XXIX. 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.

XXX. Não colocar à disposição do 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).

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

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

XXXIII. 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.

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

XXXV. Não embarçar ou frustrar a fiscalização e o acompanhamento da execução do objeto deste Termo de Contrato por servidor designado pelo contratante.

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

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

XXXVII. 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.

XXXVIII. 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.

XXXIX. 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.

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

XLI. 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.

XLII. 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.

## **CLÁUSULA QUARTA – DA DESCRIÇÃO DA SOLUÇÃO E DAS ESPECIFICAÇÕES TÉCNICAS**

A CONTRATANTE atenderá às especificações e às condições de execução dos serviços, nos termos definidos nesta cláusula.

### **§ 1º DESCRIÇÃO DA SOLUÇÃO**

I. 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).

II. 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.

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

#### **IV. Especificação técnica mínima Solução de Segurança de EndPoint**

##### **a. Servidor de Administração e Console Gerenciamento**

###### **i. Características:**

- 1.º. A console deve ser acessada via WEB (HTTPS);
- 2.º. A console deve suportar arquitetura cloud-based;
- 3.º. Console deve ser baseada no modelo cliente/servidor;
- 4.º. A console deve suportar autenticação de dois fatores;
- 5.º. Deve permitir a atribuição de perfis para os administradores da solução de Antivírus;
- 6.º. Deve permitir incluir usuários do AD para logarem na console de administração
- 7.º. 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;
- 8.º. 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;
- 9.º. Deverá ser possível buscar novos produtos e soluções a partir da console;
- 10.º. Capacidade de remover remotamente e automaticamente qualquer solução de antivírus (própria ou de terceiros) que estiver presente nas estações e servidores;
- 11.º. 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.
- 12.º. Deve registrar em arquivo de log todas as atividades efetuadas pelos administradores, permitindo execução de análises em nível de auditoria;
- 13.º. Deve armazenar histórico das alterações feitas em políticas;

14.º. 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;

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

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

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

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

19.º. 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;

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

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

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

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

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

25.º. 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;

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

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

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

29.º. Nome do computador;

30.º. Nome do domínio;

31.º. Range de IP;

32.º. Sistema Operacional;

33.º. Máquina virtual.

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

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

36.º. Pesquisa de rede (Windows pooling);

37.º. Pesquisa ativa do AD (AD pooling);

38.º. Pesquisa de IP (IP pooling);

39.º. Pesquisa de rede (Zeroconf pooling);

40.º. 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;

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

42.º. 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;

43.º. 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;

44.º. 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;

45.º. 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;

46.º. Deve fornecer as seguintes informações dos computadores:

47.º. Se o antivírus está instalado;

48.º. Se o antivírus está iniciado;

49.º. Se o antivírus está atualizado;

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

51.º. Minutos/horas desde a última atualização de vacinas;

52.º. Data e horário da última verificação executada na máquina;

53.º. Versão do antivírus instalado na máquina;

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

55.º. Quantidade de vírus encontrados (contador) na máquina;

56.º. Nome do computador;

57.º. Domínio ou grupo de trabalho do computador;

58.º. Data e horário da última atualização de vacinas;

59.º. Sistema operacional com Service Pack;

60.º. Quantidade de processadores;

61.º. Quantidade de memória RAM;

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

63.º. Endereço IP;

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

65.º. 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;

66.º. Vulnerabilidades de aplicativos instalados na máquina;

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

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

69.º. Alteração de Gateway Padrão;

70.º. Alteração de subrede;

71.º. Alteração de domínio;

72.º. Alteração de servidor DHCP;

73.º. Alteração de servidor DNS;

74.º. Alteração de servidor WINS;

75.º. Resolução de Nome;

76.º. Disponibilidade de endereço de conexão SSL;

77.º. Capacidade de configurar políticas móveis para que quando um computador cliente

---

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

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

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

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

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

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

83.º. 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;

84.º. 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;

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

86.º. Capacidade de monitoramento do sistema através de um SNMP client;

87.º. Capacidade enviar eventos através de protocolo de syslog;

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

89.º. Deve ser capaz de enviar os eventos para sistemas de SIEM em canal encriptado.

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

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

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

93.º. Deve encontrar computadores na rede através de no mínimo três formas: Domínio, Active Directory e subredes;

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

95.º. 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;

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

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

98.º. 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);

99.º. 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;

100.º. Capacidade de realizar atualização incremental de vacinas nos computadores clientes;

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

102.º. Nome do vírus; 1

103.º. Nome do arquivo infectado;

104.º. Data e hora da detecção;

105.º. Nome da máquina ou endereço IP;

106.º. Ação realizada.

107.º. Capacidade de reportar vulnerabilidades de softwares presentes nos computadores;

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

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

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

111.º. Capacidade de realizar resumo de hardware de cada máquina cliente;

112.º. Capacidade de diferenciar máquinas virtuais de máquinas físicas.

#### **b. Sistemas operacionais Windows**

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

1.º. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;

2.º. Microsoft Windows 8 Professional/Enterprise;

3.º. Microsoft Windows 8.1 Professional / Enterprise;

4.º. Microsoft Windows 10 Pro / Enterprise / Home / Education;

5.º. Microsoft Windows 11 Pro / Enterprise / Home / Education;

##### **ii. Deve ser compatível com os seguintes sistemas servidores:**

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

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

3.º. Windows Server 2016 Essentials / Standard / Datacenter;

4.º. Windows Server 2019 Essentials / Standard / Datacenter;

5.º. Windows Server 2022.

##### **iii. Suporta as seguintes plataformas virtuais:**

1.º. VMware Workstation 16.2.3;

2.º. VMware ESXi 7.0 Update 3d;

3.º. Microsoft Hyper-V Server 2019;

4.º. Citrix Hypervisor 8.2

##### **iv. Características:**

1.º. Deve prover as seguintes proteções:

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

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

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

5.º. Deve possuir módulo dedicado contra prevenção de intrusão, Prevenção de intrusão do host;

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

7.º. Controle de dispositivos externos;

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

9.º. Controle de acesso a sites por horário;

10.º. Controle de acesso a sites por usuários;

11.º. Controle de acesso a websites por dados, ex: Bloquear websites com conteúdos de

---

vídeo e áudio;

- 12.º. Controle de execução de aplicativos;
- 13.º. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
- 14.º. Capacidade de escolher quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
- 15.º. 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);
- 16.º. Capacidade de detecção de presença de antivírus de outro fabricante que possa causar incompatibilidade, bloqueando a instalação;
- 17.º. 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;
- 18.º. 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;
- 19.º. Deverá possuir módulo dedicado para proteção contra port scanning;
- 20.º. Deverá possuir módulo dedicado para proteção contra network flooding;
- 21.º. Possibilidade de desabilitar automaticamente varreduras agendadas quando o computador estiver funcionando a partir de baterias (notebooks);
- 22.º. Capacidade de pausar automaticamente varreduras agendadas caso outros aplicativos necessitem de mais recursos de memória ou processamento;
- 23.º. 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;
- 24.º. Ter a capacidade de fazer detecções por comportamento, identificando ameaças avançadas sem a necessidade de assinaturas;
- 25.º. Deverá possuir módulo para proteção contra malwares que tenta realizar criptografia de arquivos em pastas compartilhadas.
- 26.º. Deve ter a capacidade de detectar ameaças instaladas na BIOS ROM do endpoint.
- 27.º. Deverá realizar scanner de firmware em busca de rootkits.
- 28.º. Ao detectar uma ameaça, a solução deve exibir informações:
- 29.º. Do objeto SHA256;
- 30.º. Do objeto MD5.
- 31.º. Capacidade de verificar somente arquivos novos e alterados;
- 32.º. Capacidade de verificar objetos usando heurística;
- 33.º. Capacidade de agendar uma pausa na verificação;
- 34.º. Deve permitir a filtragem de conteúdo de URL avançada efetuando a classificação dos sites em categorias;
- 35.º. Capacidade de pausar automaticamente a verificação quando um aplicativo for iniciado;
- 36.º. O antivírus de arquivos, ao encontrar um objeto potencialmente perigoso, deve:
- 37.º. Perguntar o que fazer, ou;
- 38.º. Bloquear acesso ao objeto;
- 39.º. Apagar o objeto ou tentar desinfetá-lo (de acordo com a configuração pré-estabelecida pelo administrador);
- 40.º. Caso positivo de desinfecção:
- 41.º. Restaurar o objeto para uso;
- 42.º. Caso negativo de desinfecção:

- 
- 43.º.Mover para uma área de backup ou apagar (de acordo com a configuração preestabelecida pelo administrador);
- 44.º.Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
- 45.º.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;
- 46.º.Capacidade de verificação de tráfego HTTP/HTTPS e qualquer script do Windows Script Host (JavaScript, Visual Basic Script, etc);
- 47.º.Deve ser possível realizar o monitoramento das atividades de rede em tempo real, visualizando portas UDP/TCP e Tráfego de rede por aplicativo.
- 48.º.Capacidade de alterar as portas monitoradas pelos módulos de ameaças web, controle de acesso à web e e-mail;
- 49.º.Na verificação de tráfego web, caso encontrado código malicioso o programa deve:
- 50.º.Perguntar o que fazer, ou;
- 51.º.Bloquear o acesso ao objeto e mostrar uma mensagem sobre o bloqueio, ou;
- 52.º.Permitir acesso ao objeto;
- 53.º.O antivírus de web deve realizar a verificação de, no mínimo, duas maneiras diferentes, sob escolha do administrador:
- 54.º.Verificação on-the-fly, onde os dados são verificados enquanto são recebidos em tempo-real, ou;
- 55.º.Verificação de buffer, onde os dados são recebidos e armazenados para posterior verificação;
- 56.º.Possibilidade de adicionar sites da web em uma lista de exclusão, onde não serão verificados pelo antivírus de web;
- 57.º.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;
- 58.º.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;
- 59.º.Deve possuir módulo de bloqueio de Phishing, com atualizações incluídas nas vacinas, obtidas pelo Anti-Phishing Working Group (<http://www.antiphishing.org/>);
- 60.º.Capacidade de distinguir diferentes subnets e conceder opção de ativar ou não o firewall para uma subnet específica;
- 61.º.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;
- 62.º.Deve permitir a importação e exportação de listas de regras e exclusões para as aplicações no formato XML;
- 63.º.Deve permitir a criação de zonas confiáveis locais independentes por parte do usuário.
- 64.º.O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras;
- 65.º.Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
- 66.º.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.
- 67.º.Deve possuir módulo que habilite ou não o funcionamento dos seguintes dispositivos externos, no mínimo:

- 
- 68.º. Discos de armazenamento locais;
  - 69.º. Armazenamento removível;
  - 70.º. Impressoras;
  - 71.º. CD/DVD;
  - 72.º. Drives de disquete;
  - 73.º. Modems;
  - 74.º. Dispositivos de fita;
  - 75.º. Dispositivos multifuncionais;
  - 76.º. Leitores de smart card;
  - 77.º. Wi-Fi;
  - 78.º. Adaptadores de rede externos;
  - 79.º. Dispositivos MP3 ou smartphones;
  - 80.º. Dispositivos Bluetooth;
  - 81.º. Câmeras e Scanners.
  - 82.º. 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;
  - 83.º. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por usuário;
  - 84.º. Capacidade de limitar a escrita e leitura em dispositivos de armazenamento externo por agendamento;
  - 85.º. Deve permitir controlar o acesso a dispositivos externos com base em prioridade de regras.
  - 86.º. Capacidade de habilitar “logging” em dispositivos removíveis tais como Pendrive, Discos externos, etc.
  - 87.º. Capacidade de configurar novos dispositivos por Class ID/Hardware ID;
  - 88.º. 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);
  - 89.º. Ter a capacidade de detectar a modificação de firmware em dispositivos USB malintencionado.
  - 90.º. Deverá realizar a validação dos dispositivos que se conectam via USB que emulam teclados;
  - 91.º. O controle de aplicações deve ter a capacidade de criar regras seguindo os seguintes modos de operação:
  - 92.º. Black list: Permite a execução de qualquer aplicação, exceto pelas especificadas por regras.
  - 93.º. White list: Impede a execução de qualquer aplicação, exceto pelas especificadas por regras.
  - 94.º. Capacidade de bloquear execução de aplicativo que está em armazenamento externo;
  - 95.º. 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;
  - 96.º. 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;
  - 97.º. 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.

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

99.º. Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros.

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

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

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

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

### **c. Estações Mac OS X**

#### **i. Compatibilidade:**

1.º. macOS Mojave 10.14

2.º. macOS Catalina 10.15

3.º. macOS Big Sur 11.0

4.º. macOS Monterey 12

#### **ii. Características:**

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

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

3.º. Possuir módulo de bloqueio à ataques na rede;

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

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

6.º. Possibilidade de importar uma chave no pacote de instalação;

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

8.º. 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);

9.º. Capacidade de voltar para a base de dados de vacina anterior;

10.º. 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;

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

12.º. 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;

13.º. Capacidade de verificar somente arquivos novos e alterados;

14.º. Capacidade de verificar objetos usando heurística;

15.º. Capacidade de agendar uma pausa na verificação;

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

17.º. Perguntar o que fazer, ou;

18.º. Bloquear acesso ao objeto;

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

- 
- 20.º.Caso positivo de desinfecção;
  - 21.º.Restaurar o objeto para uso;
  - 22.º.Caso negativo de desinfecção;
  - 23.º.Mover para área de backup ou apagar (de acordo com a configuração pré-estabelecida pelo administrador);
  - 24.º.Anteriormente a qualquer tentativa de desinfecção ou exclusão permanente, o antivírus deve realizar um backup do objeto;
  - 25.º.Capacidade de verificar arquivos de formato de email;
  - 26.º.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;
  - 27.º.Capacidade de, através da mesma console central de gerenciamento:
  - 28.º.Ser instalado;
  - 29.º.Ser removido;
  - 30.º.Ser gerenciado;

#### **d. Sistemas operacionais Linux**

##### **i. Compatibilidade:**

##### **1.º. Plataforma 32-bits:**

- 1º.1. Red Hat Linux 6.7 e superior;
- 1º.2. CentOS 6.7 e superior;
- 1º.3. Debian 9.4 e superior;
- 1º.4. Debian 10.1 e superior;
- 1º.5. Debian 11.1 e superior;

##### **ii. Plataforma 64-bits:**

- 1.º. Ubuntu 18.04 e superior;
- 2.º. Ubuntu 20.04;
- 3.º. Red Hat Enterprise Linux 8.0;
- 4.º. CentOS 8.0 e superior;
- 5.º. Debian 10.1 e superior;
- 6.º. Oracle Linux 8.0 e superior;

##### **iii. Características:**

- 1.º. Deve prover as seguintes proteções:
- 2.º. Antivírus de arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
- 3.º. Deve permitir gerenciamento, no mínimo, das seguintes formas:
- 4.º. Via linha de comando;
- 5.º. Via console administrativa;
- 6.º. Via GUI;
- 7.º. Via web (remotamente);
- 8.º. Deve possuir funcionalidade de scan de drives removíveis, tais como:
- 9.º. CDs;
- 10.º.DVDs;
- 11.º. Discos blu-ray;
- 12.º.Flash drives (pen drives);
- 13.º.HDs externos;
- 14.º.Disquetes;
- 15.º. Deve fornecer os seguintes controles para dispositivos externos conectados ao computador:
- 16.º.Por tipo de dispositivo;

- 
- 17.º.Por barramento de conexão.
  - 18.º.As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
  - 19.º.Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
    - 20.º.Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
    - 21.º.Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
    - 22.º.Leitura de configurações;
    - 23.º.Modificação de configurações;
    - 24.º.Gerenciamento de Backup;
    - 25.º.Visualização de logs;
    - 26.º.Gerenciamento de logs;
    - 27.º.Gerenciamento de ativação da aplicação;
    - 28.º.Gerenciamento de permissões (adicionar/excluir permissões acima);
    - 29.º.Capacidade de criar exclusões por local, máscara e nome da ameaça;
    - 30.º.Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
    - 31.º.Gerenciamento de Backup: Criação de cópias dos objetos infectados em um reservatório de backup antes da tentativa de desinfetar ou remover tal objeto, sendo assim possível a restauração de objetos que contenham informações importantes;
    - 32.º.Detectar aplicações que possam ser utilizadas como vetor de ataque por hackers;
    - 33.º.Fazer detecções através de heurística utilizando no mínimo as seguintes opções de nível:
      - 34.º.Alta;
      - 35.º.Média;
      - 36.º.Baixa;
      - 37.º.Recomendado;
    - 38.º.Gerenciamento de backup de arquivos: Fazer backup de objetos suspeitos e corrompidos, salvando tais arquivos em uma pasta de backup;
    - 39.º.Verificação por agendamento: procura de arquivos infectados e suspeitos (incluindo arquivos em escopos especificados); análise de arquivos; desinfecção ou remoção de objetos infectados.
    - 40.º. Em caso erros, deve ter capacidade de criar logs automaticamente, sem necessidade de outros softwares;
    - 41.º.Capacidade de definir o consumo de recursos nas varreduras para não impactar outros aplicativos que necessitem de mais recursos de memória ou processamento;
    - 42.º.Deverá ser possível priorizar a execução de tarefas;
    - 43.º.Capacidade de verificar objetos usando heurística;
    - 44.º. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos em malicioso;
    - 45.º.Deve fornecer análise de todo o tráfego HTTP/HTTPS/FTP;
    - 46.º.O módulo de análise de tráfego deve fornecer os seguintes componentes de proteção:
    - 47.º.Detecção de phishing e sites maliciosos;
    - 48.º.Bloqueio de download de arquivos maliciosos;
    - 49.º.Bloqueio de adware;
    - 50.º.Deve possuir módulo escolha da pasta onde arquivos restaurados de backup e arquivos serão gravados;
    - 51.º.Deve fornecer a possibilidade de administração remoto através de ferramenta nativa ou Webmin (ferramenta nativa GNU-Linux).
    - 52.º.Deverá fornecer informações de todas os executáveis das aplicações;
    - 53.º.Deve possuir módulo de proteção contra criptografia maliciosa.

- 
- 54.º. Deverá possuir controle de execução de aplicações;
  - 55.º. O módulo de controle de aplicação deverá possuir as seguintes funcionalidades:
  - 56.º. Criação de lista de bloqueio de aplicação;
  - 57.º. Criação de lista de permissão de aplicação;
  - 58.º. Deverá realizar busca de ameaças em setores críticos do sistema operacional;
  - 59.º. Setor de inicialização;
  - 60.º. Objetos de inicialização;
  - 61.º. Processos de memória;
  - 62.º. Memória do kernel;
- e. Compatibilidade com servidores windows legados.**
- i. Compatibilidade de sistema legado:**
- 1.º. Plataforma x32 ou x64:
    - 1º.1. Windows Server 2003 Standard/Enterprise/Datacenter SP2 e posterior;
    - 1º.2. Windows Server 2003 R2 Standard/Enterprise/Datacenter SP2 e posterior;
- ii. Características:**
- 1.º. Deve prover as seguintes proteções:
  - 2.º. Antivírus de Arquivos residente (anti-spyware, anti-trojan, anti-malware, etc) que verifique qualquer arquivo criado, acessado ou modificado;
  - 3.º. Auto-proteção contra-ataques aos serviços/processos do antivírus;
  - 4.º. Firewall com IDS;
  - 5.º. Controle de vulnerabilidades do Windows e dos aplicativos instalados;
  - 6.º. Capacidade de escolher de quais módulos serão instalados, tanto na instalação local quanto na instalação remota;
  - 7.º. Deve permitir gerenciamento, no mínimo, das seguintes formas:
    - 8.º. Via console administrativa;
    - 9.º. Via web (remotamente);
    - 10.º. As vacinas devem ser atualizadas pelo fabricante de, no máximo, uma em uma hora;
    - 11.º. Deverá ter a capacidade de customizar o uso de CPU para realização de scanner no dispositivo.
  - 12.º. Capacidade de configurar a permissão de acesso às funções do antivírus com, no mínimo, opções para as seguintes funções:
    - 13.º. Gerenciamento de status de tarefa (iniciar, pausar, parar ou resumir tarefas);
    - 14.º. Gerenciamento de tarefa (criar ou excluir tarefas de verificação);
    - 15.º. Leitura de configurações;
    - 16.º. Modificação de configurações;
    - 17.º. Gerenciamento de backup;
    - 18.º. Visualização de logs;
    - 19.º. Gerenciamento de logs;
    - 20.º. Gerenciamento de ativação da aplicação;
    - 21.º. Gerenciamento de permissões (adicionar/excluir permissões acima);
    - 22.º. Deve possuir bloqueio de inicialização de aplicativos baseado em whitelists.
    - 23.º. O módulo de Firewall deve conter, no mínimo, dois conjuntos de regras:
    - 24.º. Filtragem de pacotes: onde o administrador poderá escolher portas, protocolos ou direções de conexão a serem bloqueadas/permitidas;
    - 25.º. 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.
    - 26.º. 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;

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

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

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

30.º. Deve possuir funcionalidade de análise personalizada de logs do Windows.

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

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

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

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

35.º. 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;

36.º. 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;

37.º. Capacidade de verificar somente arquivos novos e alterados;

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

39.º. Capacidade de verificar objetos usando heurística;

40.º. Capacidade de configurar diferentes ações para diferentes tipos de ameaças;

41.º. Capacidade de agendar uma pausa na verificação;

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

43.º. Perguntar o que fazer, ou;

44.º. Bloquear acesso ao objeto;

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

46.º. Caso positivo de desinfecção:

47.º. Restaurar o objeto para uso;

48.º. Caso negativo de desinfecção:

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

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

51.º. Possibilidade de escolha da pasta onde serão guardados os backups e arquivos maliciosos em área de backup;

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

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

54.º. Executar os procedimentos pré-configurados pelo administrador;

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

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

57.º.Bloquear atividade de malware explorando vulnerabilidades em softwares de terceiros

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

59.º. 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.

60.º.Deve possuir controle de dispositivos externos.

#### **f. Smartphones e tablets**

##### **i. Compatibilidade com Android**

1º. Android das versões: 5.0 ao 12.

##### **ii. Características:**

1.º. Deve prover as seguintes proteções:

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

3.º. Proteção contra adware e autodialers;

4.º. Todos os objetos transmitidos;

5.º. Arquivos abertos no smartphone;

6.º. Programas instalados usando a interface do smartphone

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

8.º. Deverá isolar em área de backup os arquivos infectados;

9.º. Deverá atualizar as bases de vacinas de modo agendado;

10.º.Capacidade de desativar por política:

11.º. Wi-fi;

12.º.Câmera;

13.º.Bluetooth.

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

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

16.º. Deverá ter firewall pessoal;

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

18.º.Capacidade de enviar comandos remotamente de:

19.º.Localizar;

20.º.Bloquear.

21.º.Capacidade de detectar Root nos dispositivos;

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

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

24.º.Capacidade de configurar White e blacklist de aplicativos;

25.º.Capacidade de localizar o dispositivo quando necessário;

26.º.Permitir atualização das definições quando estiver em “roaming”;

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

28.º.Capacidade de agendar uma verificação;

29.º.Capacidade de enviar URL de instalação por e-mail;

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

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

- 32.º. Deletar;
- 33.º. Ignorar;
- 34.º. Fazer backup;
- 35.º. Perguntar ao usuário.

**g. Compatibilidade com iOS:**

**i. Ser compatível com dispositivos com os sistemas operacionais:**

- 1.º. iOS 10.0 – 10.3.3
- 2.º. iOS 11.0 – 11.3
- 3.º. iOS 12.0
- 4.º. iOS 13.0
- 5.º. iPadOS 13 ao 15

**ii. Características:**

- 1.º. Capacidade de ajustar as configurações de:
- 2.º. Senha do usuário;
- 3.º. Criptografia de dados;
- 4.º. Capacidade de instalar certificados digitais em dispositivos móveis;
- 5.º. Capacidade de instalar as ferramentas necessárias para o gerenciamento dos dispositivos clientes através de:
  - 6.º. Link por e-mail;
  - 7.º. Link por mensagem de texto;
  - 8.º. QR Code
- 9.º. Capacidade de, remotamente, apagar todos os dados de dispositivos iOS;
- 10.º. Capacidade de, remotamente, bloquear um dispositivo iOS;

**h. Criptografia**

**i. Compatibilidade**

- 1.º. Microsoft Windows 7 Ultimate SP1 ou superior x86/x64;
- 2.º. Microsoft Windows 7 Enterprise SP1 ou superior x86/x64;
- 3.º. Microsoft Windows 7 Professional SP1 ou superior x86/x64;
- 4.º. Microsoft Windows 8 Enterprise x86/x64;
- 5.º. Microsoft Windows 8 Pro x86/x64;
- 6.º. Microsoft Windows 8.1 Pro x86/x64;
- 7.º. Microsoft Windows 8.1 Enterprise x86/x64;
- 8.º. Microsoft Windows 10 Enterprise x86/x64;
- 9.º. Microsoft Windows 10 Pro x86/x64;

**i. Características:**

- i. 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;
- ii. Utilizar, no mínimo, algoritmo AES com chave de 256 bits;
- iii. Capacidade de criptografar completamente o disco rígido da máquina, adicionando um ambiente de pré-boot para autenticação do usuário;
- iv. Capacidade de utilizar Single Sign-On para a autenticação de pré-boot;
- v. Permitir criar vários usuários de autenticação pré-boot;
- vi. Deve permitir que o usuário monitore a criptografia do disco ou o processo de descriptografia em tempo real;
- vii. Capacidade de criar um usuário de autenticação pré-boot comum com uma senha igual para todas as máquinas a partir da console de gerenciamento;
- viii. Capacidade de criptografar drives removíveis de acordo com regra criada pelo administrador, com as opções:
  - ix. Criptografar somente os arquivos novos que forem copiados para o disco

---

removível, sem modificar os arquivos já existentes;

- x. Criptografar todos os arquivos individualmente;
- xi. Criptografar o dispositivo inteiro, de maneira que não seja possível listar os arquivos e pastas armazenadas;
- xii. Criptografar o dispositivo em modo portátil, permitindo acessar os arquivos em máquinas de terceiros através de uma senha;
- xiii. Capacidade de selecionar pastas e arquivos (por tipo, ou extensão) para serem criptografados automaticamente;
- xiv. Capacidade de criar regras de exclusões para que certos arquivos ou pastas nunca sejam criptografados;
- xv. Capacidade de selecionar aplicações que podem ou não ter acesso aos arquivos criptografados;
- xvi. Verifica compatibilidade de hardware antes de aplicar a criptografia;
- xvii. Possibilita estabelecer parâmetros para a senha de criptografia;
- xviii. Capacidade de permitir o usuário solicitar permissão a determinado arquivo criptografado para o administrador mediante templates customizados;
- xix. Permite criar exclusões para não criptografar determinados “discos rígidos” através de uma busca por nome do computador ou nome do dispositivo
- xx. Permite criptografar as seguintes pastas pré-definidas: “meus documentos”, “Favoritos”, “Desktop”, “Arquivos temporários” e “Arquivos do outlook”;
- xxi. Permite utilizar variáveis de ambiente para criptografar pastas customizadas;
- xxii. Capacidade de criptografar arquivos por grupos de extensão, tais como: Documentos do office, Document, arquivos de audio, etc;
- xxiii. Permite criar um grupo de extensões de arquivos a serem criptografados;
- xxiv. Capacidade de criar regra de criptografia para arquivos gerados por aplicações;
- xxv. Permite criptografia de dispositivos móveis mesmo quando o endpoint não possuir comunicação com a console de gerenciamento.
- xxvi. Capacidade de deletar arquivos de forma segura após a criptografia;
- xxvii. Capacidade de criptografar somente o espaço em disco utilizado;
- xxviii. Deve ter a opção de criptografar arquivos criados a partir de aplicações selecionadas pelo administrador;
- xxix. Capacidade de bloquear aplicações selecionadas pelo administrador de acessarem arquivos criptografados;
- xxx. Deve permitir criptografar somente o espaço utilizado em dispositivos removíveis tais como pendrives, HD externo, etc;
- xxxi. Capacidade de criptografar discos utilizando a criptografia BitLocker da Microsoft;
- xxxii. Deve ter a opção de utilização de TPM para criptografia através do BitLocker;
- xxxiii. Capacidade de fazer “Hardware encryption”;

#### **j. Gerenciamento de Sistemas**

- i. Capacidade de criar imagens de sistema operacional remotamente e distribuir essas imagens para computadores gerenciados pela solução e para computadores bare-metal;
- ii. Deve possibilitar a utilização de servidores PXE na rede para deploy de imagens;
- iii. Capacidade de detectar softwares de terceiros vulneráveis, criando assim um relatório de softwares vulneráveis;
- iv. 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;
- v. Capacidade de gerenciar licenças de softwares de terceiros;

- vi. Capacidade de atualizar informações sobre hardware presentes nos relatórios após mudanças de hardware nas máquinas gerenciadas;
- vii. Possibilita fazer distribuição de software de forma manual e agendada;
- viii. Suporta modo de instalação silenciosa;
- ix. Suporte a pacotes MSI, exe, bat, cmd e outros padrões de arquivos executáveis;
- x. Possibilita fazer a distribuição através de agentes de atualização;
- xi. Utiliza tecnologia multicast para evitar tráfego na rede;
- xii. Possibilita criar um inventário centralizado de imagens;
- xiii. Capacidade de atualizar o sistema operacional direto da imagem mantendo os dados do usuário;
- xiv. Capacidade de atuar como servidor de atualização do Windows podendo fazer deploy de patches;
- xv. Suporta modo de teste, podendo atribuir alguns computadores para receberem as atualizações de forma automática para avaliação de alterações no comportamento;
- xvi. Capacidade de gerar relatórios de vulnerabilidades e patches;
- xvii. Possibilita criar exclusões para aplicação de patch por tipo de sistema operacional, Estação de trabalho e Servidor ou por grupo de administração;
- xviii. Permite iniciar instalação de patch e correções de vulnerabilidades ao reiniciar ou desligar o computador;
- xix. Permite baixar atualizações para o computador sem efetuar a instalação
- xx. Permite o administrador instalar somente atualizações aprovadas, instalar todas as atualizações (exceto as bloqueadas) ou instalar todas as atualizações incluindo as bloqueadas;
- xxi. Capacidade de instalar correções de vulnerabilidades de acordo com a severidade;
- xxii. Permite selecionar produtos a serem atualizados pela console de gerenciamento;
- xxiii. Permite selecionar categorias de atualizações para serem baixadas e instaladas, tais como: atualizações de segurança, ferramentas, drivers, etc;
- xxiv. Capacidade de adicionar caminhos específicos para procura de vulnerabilidades e updates em arquivos;
- xxv. Capacidade de instalar atualizações ou correções somente em computadores definidos, em grupos definidos ou em uma porcentagem de computadores conforme selecionado pelo administrador;
- xxvi. Capacidade de configurar o reinício do computador após a aplicação das atualizações e correções de vulnerabilidades;
- xxvii. Deve permitir selecionar o idioma das aplicações que serão atualizadas;
- xxviii. Permitir agendar o sincronismo entre a console de gerenciamento e os sites da Microsoft para baixar atualizações recentes;

## **1. Detecção e Resposta**

### **i. Compatibilidade**

- 1.º. Deve ser compatível com os seguintes sistemas de estação de trabalho:
  - 1º.1. Microsoft Windows 7 Home/Professional/Enterprise/Ultimate SP1;
  - 1º.2. Microsoft Windows 8 Professional/Enterprise;
  - 1º.3. Microsoft Windows 8.1 Professional / Enterprise;
  - 1º.4. Microsoft Windows 10 Pro / Enterprise / Home / Education;
  - 1º.5. Microsoft Windows 11 Pro / Enterprise / Home / Education;
- 2º. Deve ser compatível com os seguintes sistemas servidores:
  - 2º.1. Windows Server 2008 R2 Standard/Enterprise/Datacenter SP 1 e superior;
  - 2º.2. Windows Server 2012 e R2 Foundation / Essentials / Standard / Datacenter;
  - 2º.3. Windows Server 2016 Essentials / Standard / Datacenter;

---

2º.4. Windows Server 2019 Essentials / Standard / Datacenter;

2º.5. Windows Server 2022.

**ii. Características:**

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

2.º. A solução deve oferecer módulo focado em capacidades de EDR “Endpoint Detection and Response”, incluindo no mínimo as seguintes capacidades:

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

4.º. Deve fornecer graficamente a visualização da cadeia do ataque;

5.º. 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).

6.º. 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:

7.º. Isolar o host;

8.º. Iniciar uma varredura nas áreas críticas;

9.º. Quarentenar o objeto;

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

11.º. Visibilidade das detecções provenientes de endpoint;

12.º. Processos;

13.º. Conexões remotas;

14.º. Alterações de registros;

15.º. Objetos baixados

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

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

18.º. Deverá possuir informações de assinaturas digitais da ameaça;

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

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

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

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

23.º. Prevenir a execução de um arquivo;

24.º. Quarentenar um arquivo;

25.º. Iniciar uma varredura por IoC;

26.º. Parar um processo;

27.º. Executar um processo;

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

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

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

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

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

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

34.º. Deve oferecer informações de inteligência de ameaças do próprio fabricante;

35.º. Deverá possuir detecção baseada em sandbox do tipo cloud;

36.º. Deverá suportar IoC de terceiros em formatos OpenIOC.

**m. Especificação técnica mínima Solução de Segurança de EndPoint XDR**

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

ii. Console do módulo de detecção e reposta.

1.º Console de gerenciamento deve apresentar uma dashboard customizável.

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

3.º Deve permitir criar perfis de layout;

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

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

5.º.1. Saúde do sistema;

5.º.2. Tráfego em tempo real;

5.º.3. Mostrar alertas por importância;

5.º.4. Alertas por tecnologias de detecção;

5.º.5. Alertas por vetor de ataques;

5.º.6. Deve permitir criar novos usuários para acesso à console com pelo menos 3 níveis de acesso.

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

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

8.º Possibilidade de assinalar um evento para determinado usuário para verificação;

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

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

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

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

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

13.º.1. Status do Alerta.

13.º.2. Nível de importância.

13.º.3. Servidor em que o alerta foi criado.

13.º.4. Host em que ocorreu o ataque.

13.º.5. Fonte dos dados.

13.º.6. Hora em que o alerta foi criado.

13.º.7. Hora em que as informações do alerta foram atualizadas.

13.º.8. Nome do arquivo.

13.º.9. Tipo de arquivo.

13.º.10. Tamanho do arquivo.

13.º.11. Hash MD5 e 256 do arquivo.

13.º.12. E-mail.

13.º.13. Assunto do e-mail.

13.º.14. IP do Servidor de envio.

13.º.15. Cabeçalho.

13.º.16. Objetos Detectados.

13.º.17. URL.

13.º.18. Usuário.

14.º. Deve permitir importar IOCs (Índices de comprometimento) visando encontrar

---

ataques de acordo com informações contidas no IoC;

15.º Capacidade de executar as seguintes tarefas remotamente nos endpoints:

15º.1. Finalizar processo;

15º.2. Executar programa;

15º.3. Coletar arquivo;

15º.4. Deletar arquivo;

15º.5. Quarentenar arquivo;

15º.6. Restaurar arquivo da quarentena;

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

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

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

19.º 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;

20.º 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;

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

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

23.º Deve ser possível realizar consultas de IP, HASH domínios no portal de inteligência do próprio fabricante.

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

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

26.º Capacidade de baixar arquivos quarentenados diretamente pela console de administração;

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

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

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

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

31.º Deve permitir adicionar imagens ao relatório;

32.º Permitir criar listas brancas baseadas nos seguintes filtros:

32º.1. Por hash MD5;

32º.2. Por formato;

32º.3. Por URL;

32º.4. Por e-mail;

32º.5. Por subrede;

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

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

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

iii. Módulo de Sandbox

36.º As Sandboxes deverão suportar os seguintes sistemas operacionais:

36.º.1 Windows XP x86 Sp3;

36.º.2 Windows 7 X64;

36.º.3 Windows 10 x64;

36.º.4 CentOS 7.8.

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

38.º 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;

39.º 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:

39.º.1 URLs/sites web relacionados ao ataque,

39.º.2 hashes MD5

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

41.º Arquivos executáveis;

42.º Scripts;

43.º Arquivos;

44.º Documentos do office;

45.º Arquivos de mídia;

46.º Arquivos de Android (APK)

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

48.º Suportar mecanismo de whitelist pelos seguintes métodos:

48.º.1. Hash MD5 do arquivo;

48.º.2 Formato do arquivo;

48.º.3 E-mail;

48.º.4 Subrede.

48.º.5 Deve permitir o envio de alertas por e-mail;

49.º. 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;

50.º. Capacidade de instalar imagens customizadas do Windows para analisar objetos na Sandbox.

V. Garantia e suporte técnico a Durante 60 (sessenta) meses,

a Contratada deverá prover a garantia, manutenção e suporte técnico.

b 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.

c 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.

d 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.

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

f O Suporte Técnico engloba as seguintes atividades:

- i. Identificação e resolução de falhas na solução.
- ii. Assistência na instalação de licenças/agentes.
- iii. Auxílio na operação da console de gerenciamento.
- iv. Abordagem de problemas de disponibilidade dos serviços contratados.
- v. Qualquer outro suporte relacionado aos serviços contratados.

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

h 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.

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

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

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

l 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.

m 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.

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

- i. Data e hora da abertura do chamado.
- ii. Identificação do requisitante da abertura do chamado.
- iii. Identificação do número do contrato.
- iv. Descrição do serviço/ocorrência.
- v. Identificação da severidade do serviço/ocorrência.
- vi. Identificação do atendente da Contratada responsável pelo registro do chamado.

o 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.

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

i. 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.

ii. 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.

q 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.

r 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.

s 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.

t 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.

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

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

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

x 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.

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

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

aa 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.

bb 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.

cc 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.

dd 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.

ee 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.

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

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

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

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

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

#### **VI. Treinamento**

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

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

c 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.

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

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

f O treinamento será ministrado em idioma português.

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

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

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

j 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.

#### **VII. Implantação**

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

i. 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.

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

iii. 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.

iv. Instalação do software agente nos dispositivos endpoints.

b 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.

c A Contratada deverá realizar os seguintes serviços:

- i. Implementação, configuração e implantação completa da solução, incluindo a transferência de conhecimentos relacionados à operacionalização das ferramentas da solução.
- ii. Transferência de conhecimento operacional abrangendo todas as funcionalidades da solução para a equipe técnica da Contratante.
- iii. Configuração das regras de segurança e grupos, aderindo às melhores práticas de segurança e seguindo as diretrizes previamente definidas pela equipe técnica da Contratante.
- iv. 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.

## **§ 2º ESPECIFICAÇÃO TÉCNICA**

I Conforme consta no ANEXO I do Edital.

## **§ 3º MODELO DE EXECUÇÃO DO OBJETO**

I 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.

a. 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. II A execução do objeto seguirá a seguinte dinâmica:

### **a. Entrega das licenças.**

i. A contratada deverá disponibilizar as licenças de uso de software em sítio oficial do fabricante, conforme descritivo técnico especificado no item 3.4 do Anexo I do Edital, 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 do Anexo I do Edital.

ii. 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.

iii. 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.

### **b. Implantação.**

i. 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. do Anexo I do Edital com todos os requisitos descritos no item 3.7 do Anexo I do Edital atendidos e documentados em um relatório de implantação.

ii. 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.

iii. 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.

### **c. Treinamento.**

i. 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.

ii. 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.

iii. 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.

iv. 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.

v. 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.

vi. 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.

#### **CLÁUSULA QUINTA – DO PREÇO, PRAZO E CONDIÇÕES DE PAGAMENTO**

A CONTRATANTE pagará à CONTRATADA, pelos serviços prestados, o valor global anual de **R\$ 2.890.000,00 (dois milhões, oitocentos e noventa mil reais)**, referente aos serviços descritos no Anexo deste Termo de Contrato.

§ 1º A CONTRATADA deverá observar, quanto aos prazos, custo e forma de pagamento, as seguintes diretrizes:

I Os pagamentos serão realizados através de depósito bancário, preferencialmente nas agências do BANCO BRADESCO S/A, em até 30 (trinta) dias após o recebimento mensal e definitivo do objeto constante de cada uma das etapas definidas Cronograma de Execução e entregáveis, mediante apresentação de fatura/nota fiscal, em conformidade com as medições realizadas, 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.

II 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.

III 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.

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

V Os valores da(s) NF(s) / Fatura(s) deverão ser os mesmos consignados na Nota de Empenho, sem o que não será liberado o respectivo pagamento. Em caso de divergência, será estabelecido prazo para a CONTRATADA fazer a substituição desta(s) NF(s) / Fatura(s).

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

VII 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.

VIII 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.

IX 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.

X 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

XI 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.

XII Essa(s) nota(s) fiscal(is) /fatura(s) deverá(ão) ser emitida(s) em nome do Tribunal de Justiça do Estado do Ceará, CNPJ N.º 09.444.530/0001-01 e estar em conformidade com a(s) nota(s) de empenho emitida(s) pelo TJCE.

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

XIV 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.

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

XVI A CONTRATADA se obriga a manter as condições de habilitação e qualificação exigidas na contratação. 2 Nos casos de eventuais atrasos de pagamento, desde que a CONTRATADA não tenha concorrido de alguma forma para tanto, fica convencionado que a taxa de compensação financeira devida pelo CONTRATANTE, entre a data do vencimento e o efetivo adimplemento da parcela, será calculada mediante a aplicação da seguinte fórmula:

**EM = I x N x VP**, sendo:

EM = Encargos Moratórios;

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

VP = Valor da parcela a ser paga.

I = Índice de compensação financeira = 0,00016438, assim apurado:

$$I = \frac{i}{365}$$

$$I = \frac{6/100}{365}$$

$$I = 0,00016438$$

no qual  $i$  = taxa percentual anual no valor de 6% (seis por cento).

### CLÁUSULA SEXTA – DO REAJUSTE E DOS RECURSOS ORÇAMENTÁRIOS

A CONTRATANTE atenderá às prescrições para reajustamento do contrato nos termos definidos nesta cláusula.

§ 1º Os preços inicialmente contratados são fixos e irrevogáveis no prazo de um ano contado da data de apresentação da proposta.

§ 2º Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pelo CONTRATANTE, do Índice de Custo da Tecnologia da Informação (ICTI) - Ipea, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

§ 3º O processo referente ao pedido de reajuste supra, deverá ser aberto, em tempo hábil, pelo Fiscal do Contrato e firmado pelo Gestor.

§ 4º Os recursos financeiros correrão por conta do Fundo Especial de Reparelhamento e Modernização do Poder Judiciário do Estado do Ceará – FERMOJU, tendo como fonte os Recursos Diretamente Arrecadados, nas seguintes dotações orçamentárias:

**04200021.02.126.192.11470.15.449040.1.759.1200070.1.20**

**04200021.02.126.192.11470.15.449040.2.759.1200070.1.20**

**04200021.02.126.192.11473.15.449040.1.759.1200070.1.20**

**04200021.02.126.192.11473.15.449040.2.759.1200070.1.20**

§ 5º Nenhuma contratação será efetuada sem a prévia indicação da disponibilidade orçamentária.

### CLÁUSULA SÉTIMA – DOS ELEMENTOS PARA GESTÃO DO CONTRATO

Os elementos para a gestão do contrato serão processados da seguinte forma:

§ 1º 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 do ANEXO I do Edital.
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 ANEXO I do Edital.

### § 2º Prazos e Condições

I. 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 do ANEXO I do Edital 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 do ANEXO I do Edital 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 do ANEXO I do Edital 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

### § 3º Estimativa do Volume de Bens/Serviço

I Conforme item 1.2 do ANEXO I do Edital.

### § 4º Propriedade, sigilo e restrições

I 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 presente contratação, em papel ou em mídia eletrônica, sendo vedada sua cessão, locação ou venda a terceiros.

II 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.

III 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.

IV 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.

V 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 **ANEXO I - TERMO DE CIÊNCIA**, bem como a assinatura do **ANEXO II - 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.

VI 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 constante no Termo de Contrato.

#### § 5º 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 correspondência.	Contratante	Contratada	Comunicação formal	Sempre que houver falha no atendimento a 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 ( <i>Portable Document Format</i> ): documento em formato portátil.	Quando necessário

### CLÁUSULA OITAVA – DA GARANTIA DOS SERVIÇOS

A especificação da garantia do serviço deverá observar o art. 40, §1º, inciso III, da Lei nº 14.133, de 2021.

§ 1º A garantia contratual dos serviços, complementar à garantia legal, deve atender as especificações técnicas dos **itens 3.4.12 e 3.5 do ANEXO I do Edital**, pelo prazo mínimo contratual de 60 (sessenta) meses, contado a partir do primeiro dia útil subsequente à data do TRD.

### CLÁUSULA NONA – DA GARANTIA CONTRATUAL

A Adjudicatária deverá oferecer, a título de garantia do contrato, a partir da data de homologação, e conforme o Art. 98, da Lei nº 14.133/2021 e suas alterações, 5% (cinco por cento) do valor anual do contrato, devidamente atualizado.

§ 1º Será concedido prazo mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para a prestação da garantia pelo contratado quando optar pela modalidade seguro garantia. As demais modalidades deverão ser apresentadas em até 5 (cinco) dias, a contar da assinatura do Termo de Homologação.

§ 2º A garantia prestada será restituída e/ou liberada **90 (noventa) dias** após o

término da vigência contratual, desde que cumpridas integralmente todas as obrigações contratuais; quando em dinheiro, será atualizada monetariamente, conforme dispõe o art. 100, da Lei nº. 14.133/2021.

§ 3º Poderá o contratado optar por caução em dinheiro ou títulos da dívida pública, seguro-garantia ou fiança bancária, nos termos do art. 96, § 1º, da Lei 14.133/2021.

§ 4º A validade da garantia, qualquer que seja a modalidade escolhida, deverá abranger um período de 90 dias após o 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 financeira fiadora.

§ 5º Caso utilizada a modalidade de seguro-garantia, a apólice permanecerá em vigor mesmo que o contratado não pague o prêmio nas datas convencionadas.

§ 6º A garantia assegurará, qualquer que seja a modalidade escolhida, o pagamento de:

I Prejuízos advindos do não cumprimento do objeto do contrato e do não adimplemento das demais obrigações nele previstas;

II Prejuízos diretos causados à Administração, decorrentes de culpa ou dolo durante a execução do contrato;

III Multas moratórias e punitivas aplicadas pela Administração à CONTRATADA;

IV Obrigações trabalhistas e previdenciárias de qualquer natureza e para com o FGTS, não adimplidas pela CONTRATADA, quando couber.

§ 7º No caso de alteração do valor do contrato, ou prorrogação de sua vigência, a garantia deverá ser ajustada à nova situação ou renovada, seguindo os mesmos parâmetros utilizados quando da contratação.

§ 8º Se o valor da garantia for utilizado total ou parcialmente em pagamento de qualquer obrigação, a CONTRATADA obriga-se a fazer a respectiva reposição no prazo máximo de 10 (dez) dias úteis, contados da data em que for notificada.

I 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.

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

§ 9º O CONTRATANTE executará a garantia na forma prevista na legislação que rege a matéria.

§ 10 O emitente da garantia ofertada pela contratada deverá ser notificado pelo contratante quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais (art. 137, § 4º, da Lei n.º 14.133, de 2021).

§ 11 Caso se trate da modalidade seguro-garantia, ocorrido o sinistro durante a vigência da apólice, sua caracterização e comunicação poderão ocorrer fora desta vigência, não caracterizando fato que justifique a negativa do sinistro, desde que respeitados os prazos prescricionais aplicados ao contrato de seguro, nos termos do art. 20 da Circular Susep nº 662, de 11 de abril de 2022.

§ 12 Extinguir-se-á a garantia com a restituição da apólice, carta fiança ou autorização para a liberação de importâncias depositadas em dinheiro a título de garantia, acompanhada de declaração do CONTRATANTE, mediante termo circunstanciado, de que a contratada cumpriu todas as cláusulas do contrato;

§ 13 A garantia somente será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, será atualizada monetariamente.

§ 14 A garantia somente será liberada ante a comprovação de que o contratado pagou

todas as verbas rescisórias decorrentes da contratação, sendo que, caso esse pagamento não ocorra até o fim do segundo mês após o encerramento da vigência contratual, a garantia deverá ser utilizada para o pagamento dessas verbas trabalhistas, incluindo suas repercussões previdenciárias e relativas ao FGTS, observada a legislação que rege a matéria;

§ 15 Também poderá haver liberação da garantia se a empresa comprovar que os empregados serão realocados em outra atividade de prestação de serviços, sem que ocorra a interrupção do contrato de trabalho;

§ 16 Por ocasião do encerramento da prestação dos serviços contratados, a Administração Contratante poderá utilizar o valor da garantia prestada para o pagamento direto aos trabalhadores vinculados ao contrato no caso da não comprovação: (1) do pagamento das respectivas verbas rescisórias ou (2) da realocação dos trabalhadores em outra atividade de prestação de serviços.

§ 17 O garantidor não é parte para figurar em processo administrativo instaurado pelo CONTRATANTE com o objetivo de apurar prejuízos e/ou aplicar sanções à CONTRATADA.

§ 18 A CONTRATADA autoriza o CONTRATANTE a reter, a qualquer tempo, a garantia, na forma prevista no Contrato.

## **CLÁUSULA DEZ – DAS SANÇÕES ADMINISTRATIVAS**

Quanto às sanções administrativas, deve-se observar o disposto nesta cláusula.

§ 1º Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a contratado que:

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

II salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial quando:

a não enviar a proposta ajustada após a negociação;

b recusar-se a enviar o detalhamento da proposta quando exigível;

c pedir para ser desclassificado quando encerrada a etapa competitiva;

d deixar de apresentar amostra, quando exigível.

III 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.

IV 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.

V apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

VI fraudar a licitação.

VII comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

a agir em conluio ou em desconformidade com a lei;

b induzir deliberadamente a erro no julgamento;

c apresentar amostra falsificada ou deteriorada;

d praticar atos ilícitos com vistas a frustrar os objetivos da contratação; e praticar ato lesivo previsto no art. 5º da Lei 12.846/2013.

VIII 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 IV, 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.

IX 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:

a advertência;

b multa;

c impedimento de licitar e contratar; e

d 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.

X Na aplicação das sanções serão considerados:

a a natureza e a gravidade da infração cometida;

b as peculiaridades do caso concreto;

c as circunstâncias agravantes ou atenuantes;

d os danos que dela provierem para a Administração Pública;

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

XI 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.

a 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.

i Para as condutas descritas nos itens V, VI e VII, será aplicada multa de 30%.

ii Caso a Contratada não cumpra os prazos estabelecidos nos níveis de serviços, sem justificativa aceita, conforme descrito no item 3.5.19 do Anexo I do Edital, 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.

iii 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 do Anexo I do Edital, a Contratada ficará sujeita a aplicação da multa, no valor de 0,5%, acrescida de 0,1% por dia de atraso. 1º. Após o décimo dia de atraso injustificado, o Contratante poderá rescindir o contrato.

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

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

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

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

XII 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.

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

XIVA sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens I, II e III, 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.

XV Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens IV, V, VI e VII, bem como pelas infrações administrativas previstas nos itens I, II e III 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.

XVI A apuração de responsabilidades 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.

XVII 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.

XVIII 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.

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

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

XXI Sempre que houver irregularidade na prestação dos serviços executados, o CONTRATANTE efetuará a apuração das ocorrências e comunicará à CONTRATADA, conforme especificado.

XXII 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.

XXIII 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.

## **CLÁUSULA ONZE – DA EXTINÇÃO CONTRATUAL**

O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.

§ 1º Se as obrigações não forem cumpridas no prazo estipulado, a vigência ficará prorrogada até a conclusão do objeto, caso em que deverá a Administração providenciar a readequação do cronograma fixado para o contrato.

§ 2º Quando a não conclusão do contrato referida no parágrafo anterior decorrer de culpa da CONTRATADA:

I Ficará ela constituída em mora, sendo-lhe aplicáveis as respectivas sanções administrativas;

II Poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

§ 3º O contrato poderá ser extinto antes de cumpridas as obrigações nele estipuladas, ou antes do prazo nele fixado, por algum dos motivos previstos no artigo 137 da Lei nº 14.133/21, bem como amigavelmente, assegurados o contraditório e a ampla defesa.

I Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

II A alteração social ou a modificação da finalidade ou da estrutura da empresa não ensejará a extinção se não restringir sua capacidade de concluir o contrato.

III Se a operação implicar mudança da pessoa jurídica contratada, deverá ser formalizado termo aditivo para alteração subjetiva.

§ 4º A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório (art. 131, caput, da Lei nº 14.133, de 2021).

§ 5º O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei nº 14.133, de 2021).

## **CLÁUSULA DOZE – DA SUBCONTRATAÇÃO**

Não será permitida a subcontratação total ou parcial do objeto deste Termo de Contrato.

§ 1º 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.

## **CLÁUSULA TREZE – DOS CRITÉRIOS AMBIENTAIS**

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 nº 01, de 18/03/2010, da Lei nº 12.305, de 2010 – Política Nacional de Resíduos Sólidos, Resolução CONAMA nº 416, de 30/09/2009, e legislação correlata.

§ 1º 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 nº 14.133/21.

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

§ 3º 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.

§ 4º 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).

§ 5º 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 pelo CONTRATANTE.

#### **CLÁUSULA QUATORZE - DO PRAZO DE VIGÊNCIA DO CONTRATO**

O prazo de vigência deste termo de contrato será de 12 (doze) meses, contados da assinatura do CONTRATO, podendo ser prorrogado até limite permitido pela Lei 14.133/21, e conforme a conveniência estabelecida entre CONTRATADA e CONTRATANTE.

#### **CLÁUSULA QUINZE - DO GESTOR DO CONTRATO E DO ORDENADOR DE DESPESAS**

O órgão responsável pela contratação é o Tribunal de Justiça do Estado do Ceará.

§ 1º O Gestor do Contrato será a(o) Secretária(o) de Tecnologia da Informação do TJCE ou profissional por ela(e) indicado devidamente oficializado por meio de publicação no Diário da Justiça Eletrônico.

§ 2º Os Ordenadores de Despesas serão o(a) Desembargador(a) Presidente do Tribunal de Justiça do Estado do Ceará conjuntamente com a(o) Secretária(o) de Tecnologia da Informação do TJCE, conforme Portaria n. 310/2023, disponibilizada no DJe de 09 de fevereiro de 2023, que dispõe sobre a delegação de competências administrativas no âmbito do Poder Judiciário do Estado do Ceará.

#### **CLÁUSULA DEZESSEIS – DAS ALTERAÇÕES CONTRATUAIS**

As alterações ao presente contrato poderão ser necessárias se ocorrerem quaisquer das situações previstas no artigo 124 da Lei Federal nº 14.133/21.

**PARÁGRAFO ÚNICO** – A CONTRATADA deverá aceitar, nas mesmas condições propostas, os acréscimos ou as supressões que se fizerem necessária, até o limite de 25% do valor inicial do contrato, nos termos do artigo 125 da Lei nº 14.133/21.

#### **CLÁUSULA DEZESSETE – DA LEGISLAÇÃO APLICÁVEL**

Este termo de contrato rege-se pela Lei nº 14.133/21 e suas alterações, pela legislação correlata, medidas provisórias, bem como pelos preceitos de Direito Público, regulamentos, instruções normativas e ordens de fornecimento, emanados de órgãos públicos, aplicando-se-lhes, supletivamente, nos casos omissos, os princípios gerais dos contratos e demais disposições de Direito Privado.

#### **CLÁUSULA DEZOITO – DA POSSIBILIDADE DO PETICIONAMENTO PELO PORTAL DO TJCE**

Em caso de eventuais demandas da contratada, o novo Portal de Atendimento do TJCE para protocolo exclusivamente administrativo (CPA) permitirá consultas processuais, petições iniciais e intermediárias no âmbito dos processos administrativos, desde que realize cadastro prévio no Portal (<https://portaladmin.tjce.jus.br/atendimento/>) e possua certificado digital.

Visando a facilitar a utilização do Portal, foram disponibilizados 3 (três) vídeos tutoriais, cujos links seguem abaixo:

- 1) Cadastro de Usuário:  
<https://www.youtube.com/watch?v=J00Yow2ywRc>
- 2) Peticionamento Inicial:  
<https://www.youtube.com/watch?v=TNhHA6vQKdg>
- 3) Peticionamento Intermediário:  
<https://www.youtube.com/watch?v=dT5pLHNwXyw>

Os vídeos tutoriais referenciados constarão do site do TJCE (<https://www.tjce.jus.br/>) de forma permanente.

## CLÁUSULA DEZENOVE – DO FORO

Fica eleito o foro de Fortaleza (CE), para dirimir quaisquer dúvidas oriundas do presente Termo de Contrato, caso não possam ser resolvidos por via administrativa, com renúncia de qualquer outro por mais privilegiado que seja.

**PARÁGRAFO ÚNICO** - Firmam o presente em 2 (duas) vias de igual teor e forma, por estarem justos e acertados, na presença da(s) testemunha(s) que também o assinam, para que produza seus jurídicos e legais efeitos, devendo seu extrato ser publicado no Diário da Justiça Eletrônico (DJe).

Fortaleza/CE, DATA DA ÚLTIMA ASSINATURA REGISTRADA PELO SISTEMA.

**ANTONIO ABELARDO BENEVIDES MORAES:1161329730**  
Assinado de forma digital por ANTONIO ABELARDO BENEVIDES MORAES:1161329730  
Dados: 2024.10.15 11:09:09 -03'00'  
**ANTÔNIO ABELARDO BENEVIDES MORAES**  
**DESEMBARGADOR PRESIDENTE DO TJCE**

**DENISE MARIA NOROES OLSEN:28381610320**  
Assinado de forma digital por DENISE MARIA NOROES OLSEN:28381610320  
Dados: 2024.10.15 10:54:58 -03'00'

**DENISE MARIA NORÕES OLSEN**  
**SECRETÁRIA DE TECNOLOGIA DA INFORMAÇÃO DO TJCE**



**YURE LEOPOLDO SABINO DE FREITAS**  
**REPRESENTANTE DA EMPRESA NETWORK SECURE SEGURANÇA DA**  
**INFORMAÇÃO LTDA.**

**ANEXO I DO CONTRATO**  
**TERMO DE CIÊNCIA**

**INTRODUÇÃO**

Visa obter o comprometimento formal dos empregados da CONTRATADA diretamente envolvidos no \_\_\_\_\_ sobre o conhecimento da declaração de manutenção de sigilo e das normas de segurança vigentes na Instituição.

**IDENTIFICAÇÃO**

Contrato N°:			
Objeto:			
Contratante:			
Gestor do Contrato:		Matr.:	
Contratada:		CNPJ:	
Preposto da Contratada:		CPF:	

Por este instrumento, os funcionários abaixo-assinados declaram ter ciência e conhecer o teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes no CONTRATANTE.

**CIÊNCIA**

**CONTRATADA – Funcionários**

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_  
<Nome>  
Matrícula: <Matr.>

\_\_\_\_\_, de \_\_\_\_\_ de 20\_\_\_\_\_.

## **ANEXO II DO CONTRATO** **TERMO DE COMPROMISSO**

### **ANEXO II - TERMO DE COMPROMISSO – TC**

O TRIBUNAL DE JUSTIÇA DO CEARÁ, sediado em Av. General Afonso Albuquerque Lima, S/N. – Cambéba, Fortaleza-CE CEP:60822-325 – Fone: (85) 3207-7000, CNPJ nº 09.444.530/0001-01, doravante denominado CONTRATANTE, e, de outro lado, a \_\_\_\_\_, sediada em \_\_\_\_\_, nº \_\_\_\_\_, \_\_\_\_\_, \_\_\_\_\_/\_\_\_\_, CEP: \_\_\_\_-\_\_\_\_, CNPJ nº \_\_\_\_-\_\_\_\_/\_\_\_\_-\_\_\_\_, doravante denominada CONTRATADA;

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

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

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

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

#### **Cláusula Primeira – DO OBJETO**

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pelo CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

#### **Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES**

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

**INFORMAÇÃO:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

**INFORMAÇÃO SIGILOSA:** aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

**CONTRATO PRINCIPAL:** contrato celebrado entre as partes, ao qual este TERMO se vincula.

#### **Cláusula Terceira – DA INFORMAÇÃO SIGILOSA**

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte

de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades do CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

#### **Cláusula Quarta – DOS LIMITES DO SIGILO**

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

**I** – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

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

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

#### **Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES**

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

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

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

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

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa do CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pelo CONTRATANTE.

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

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

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas,

representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

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

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

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

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

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

#### **Cláusula Sexta – DA VIGÊNCIA**

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

#### **Cláusula Sétima – DAS PENALIDADES**

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pelo CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº. 14.133/21.

#### **Cláusula Oitava – DISPOSIÇÕES GERAIS**

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

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

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

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

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

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

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

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

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

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

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

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

#### **Cláusula Nona – DO FORO**

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

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

#### **DE ACORDO**

<b>CONTRATANTE</b>	<b>CONTRATADA</b>

_____	_____
Matrícula:	Representante Legal
<b>Testemunhas</b>	
<b>Testemunha 1</b>	<b>Testemunha 2</b>
_____	_____
Preposto da Contratada	Fiscal Técnico

\_\_\_\_\_, \_\_\_\_\_ de \_\_\_\_\_ de 20\_\_\_\_

**ANEXO III DO CONTRATO  
PROPOSTA DA CONTRATADA**

Ao  
TRIBUNAL DE JUSTIÇA DO ESTADO DO CEARÁ  
COMISSÃO DE LICITAÇÃO  
Ref. PREGÃO N. 028/2024  
PROCESSO N. 8510187-89.2024.8.06.0000

**Objeto:** 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 e demais especificações e características consignados, incluindo suporte e garantia pelo período de 60 meses, sob regime de empreitada por preço unitário, conforme especificações, quantitativos e exigências estabelecidas neste edital e seus anexos.

### ANEXO 3 DO EDITAL – APRESENTAÇÃO DA PROPOSTA

#### DADOS DA EMPRESA:

**Nome Empresa:** NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA  
**CNPJ:** 05.250.796/0001-54  
**Insc. Est.:** 06.180540-8  
**Endereço Comercial:** Av. Dom Manuel, 1020 - Sala 02 - Bairro: Centro  
**Cidade:** Fortaleza  
**Estado:** Ceará  
**CEP:** 60060-090  
**Telefone:** (85) 3195-2200  
**E-mail:** licitacoes@networksecure.com

#### DADOS DO REPRESENTANTE LEGAL:

**Nome:** Yure Leopoldo Sabino de Freitas  
**Função:** Diretor Comercial  
**CPF:** 525.285.023-20  
**Tel.:** (85) 3195-2200  
**Endereço Eletrônico (e-mail):** [licitacoes@networksecure.com.br](mailto:licitacoes@networksecure.com.br)

#### DADOS BANCÁRIOS

Banco: Brasil      Agência: 3515-7      Conta: 7028-9

Em atendimento ao Edital do Pregão em epígrafe, apresentamos a seguinte proposta de preços:

#### PLANILHA DE PREÇOS

ID	Objeto	QTD Licenças	Valor Unitário	Valor Total
1	Solução de Segurança de EndPoint EDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses -	10.000	R\$ 190,03	R\$ 1.900.300,00

	Kaspersky Next EDR Optimum Brazilian Edition Plus License – 5 anos licenciamento; conforme especificações do edital.			
2	Solução de Segurança de EndPoint XDR, com manutenção, garantia (update e upgrade), e suporte do fabricante por 60 meses - Kaspersky Next EDR Expert Brazilian Edition Plus License – 5 ano de licenciamento; conforme especificações do edital.	2.000	R\$ 398,97	R\$ 797.940,00
3	Serviços de instalação, configuração e implantação da solução; conforme especificações do edital.	1	R\$ 137.027,00	R\$ 137.027,00
4	Treinamento; conforme especificações do edital.	1	R\$ 54.733,00	R\$ 54.733,00
<b>Valor total</b>				<b>R\$ 2.890.000,00</b>
<b>Dois milhões e oitocentos e noventa mil reais</b>				

No valor proposto está incluso todos e quaisquer encargos e outros custos inerentes ao fornecimento do objeto da licitação, tais como: garantias, tributos, taxas, encargos sociais, trabalhistas, remunerações, materiais e equipamentos para a execução dos serviços e outros que incidam direta e indiretamente sobre o integral e perfeito cumprimento da proposta comercial apresentada.

**PRAZO DE VALIDADE DESTA PROPOSTA COMERCIAL:** 90 (noventa) dias.

Fortaleza/CE, 26 de agosto de 2024

**YURE LEOPOLDO**  
**SABINO DE**  
**FREITAS**

Assinado de forma digital  
por YURE LEOPOLDO  
SABINO DE FREITAS  
Dados: 2024.08.26 11:21:11  
-03'00'

**NETWORK SECURE SEGURANÇA DA INFORMAÇÃO LTDA**  
**CNPJ 05.250.796/0001-54**  
**YURE LEOPOLDO SABINO DE FREITAS**  
**CPF Nº: 525.285.023-20**  
**DIRETOR COMERCIAL**

---

**ANEXO IV DO CONTRATO**

**FICHA DE DADOS DO REPRESENTANTE LEGAL**

Dados pessoais do(s) representante(s) e/ou procurador(es), devidamente habilitados, da futura CONTRATADA, indicado(s) para assinatura do Termo de Contrato:

NOME : Yure Leopoldo Sabino de Freitas

NACIONALIDADE : Brasileiro

ESTADO CIVIL : Casado

PROFISSÃO : Diretor Comercia

RG : 559056187 SSP/SP

CPF : 525.285.023-20

DOMICÍLIO : Av. Dom Manuel, nº 1020

CIDADE : Fortaleza

UF : CE

FONE : (85) 3195-2200

CELULAR :

E-MAIL : licitacoes@networksecure.com.br