CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO GRANDE DO NORTE

AVISO DE DISPENSA ELETRÔNICA

Aviso de DISPENSA ELETRÔNICA Nº 8/2026

OBJETO	**AQUISIÇÃO DE 68 LICENÇAS DO ANTIVÍRUS KASPERSKY NEXT EDR FOUNDATIONS BRAZILIAN EDITION, INCLUINDO ATUALIZAÇÕES, GARANTIA E SUPORTE TÉCNICO PELO PERÍODO DE 12 (DOZE) MESES.**

PERÍODO DE PROPOSTAS De 16/**03/2026** às **8h** Até 19/**03/2026** às **8h**	**PERÍODO DE LANCES** De 19/**03/2026** às **8h** Até 19/**03/2026** às **14h**

VALOR TOTAL DA CONTRATAÇÃO	**R$ 10.860,28 (dez mil oitocentos e sessenta reais e vinte e oito centavos)**
Endereço Eletrônico	https://www.gov.br/compras/

CONDIÇÕES GERAIS DA CONTRATAÇÃO

O Conselho Regional de Medicina do Rio Grande do Norte (UASG 389178) torna pública a realização da Dispensa Eletrônica, com critério de julgamento MENOR PREÇO, na hipótese do inciso II do art. 75 da Lei nº 14.133/2021 e demais legislações aplicáveis. A participação se dará mediante Sistema de Dispensa Eletrônica integrante do Sistema de Compras do Governo Federal – ComprasNet 4.0, disponível no endereço eletrônico: https://www.gov.br/compras/pt-br/. O envio de propostas e lances deverá ocorrer, exclusivamente, por meio desse sistema eletrônico.

Conselho Regional de Medicina do Rio Grande do Norte

AVISO DE DISPENSA ELETRÔNICA Nº 8/2026
(Processo Administrativo SEI nº 26.20.000000447-7)

Torna-se público que o CONSELHO REGIONAL DE MEDICINA DO RN realizará Dispensa Eletrônica, com critério de julgamento (menor preço), na hipótese do art. 75, inciso II, nos termos da Lei nº 14.133, de 1º de abril de 2021, da Instrução Normativa SEGES/ME nº 67/2021 e demais legislação aplicável.

Data da sessão: 19**/03/2026**
Link: https://www.gov.br/compras/
Horário da Fase de Lances: 8:00 às 14:00

1. OBJETO DA CONTRATAÇÃO DIRETA

O objeto da presente dispensa é a escolha da proposta mais vantajosa para renovação/aquisição de **68**(sessenta e oito) licenças do antivírus Kaspersky Next EDR Foundations Brazilian Edition, incluindo atualizações, garantia e suporte técnico pelo período de **12**(doze) meses para continuar cobrindo com a presente solução a demanda de segurança da informação do CREMERN.

1.1. A contratação ocorrerá em item/lote único**,** conforme tabela constante abaixo.

LOTE	ITEM	DESCRIÇÃO/ ESPECIFICAÇÃO	CATSER/ CATMAT	UNIDADE DE MEDIDA	QUANT	PREÇO UNITÁRIO	PREÇO ESTIMADO total
ÚNICO	1	licenças do antivírus Kaspersky Next EDR Foundations Brazilian Edition	27502	UNIDADE	68	R$ 159,71	R$ 10.860,28

1.1.1. Havendo mais de item ou lote faculta-se ao fornecedor a participação em quantos forem de seu interesse. Entretanto, optando-se por participar de um lote, deve o fornecedor enviar proposta para todos os itens que o compõem.

1.2. O critério de julgamento adotado será o ***menor preço***, observadas as exigências contidas neste Aviso de Contratação Direta e seus Anexos quanto às especificações do objeto.

PARTICIPAÇÃO NA DISPENSA ELETRÔNICA.

1.3. A participação na presente dispensa eletrônica se dará mediante Sistema de Dispensa Eletrônica integrante do Sistema de Compras do Governo Federal – Comprasnet 4.0, disponível no endereço eletrônico https://www.gov.br/compras/.

1.3.1. Os fornecedores deverão atender aos procedimentos previstos no Manual do Sistema de Dispensa Eletrônica, disponível no Portal de Compras do Governo Federal, para acesso ao sistema e operacionalização.

1.3.2. O fornecedor é o responsável por qualquer transação efetuada diretamente ou por seu representante no Sistema de Dispensa Eletrônica, não cabendo ao provedor do Sistema ou ao órgão entidade promotor do procedimento a responsabilidade por eventuais danos decorrentes de uso indevido da senha, ainda que por terceiros não autorizados.

1.4. Não poderão participar desta dispensa os fornecedores:

1.4.1. que não atendam às condições deste Aviso de Contratação Direta e seu(s) anexo(s);

1.4.2. estrangeiros que não tenham representação legal no Brasil com poderes expressos para receber citação e responder administrativa ou judicialmente;

1.4.3. que se enquadrem nas seguintes vedações:

a) autor do anteprojeto, do projeto básico ou do projeto executivo, pessoa física ou jurídica, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ele relacionados;

b) empresa, isoladamente ou em consórcio, responsável pela elaboração do projeto básico ou do projeto executivo, ou empresa da qual o autor do projeto seja dirigente, gerente, controlador, acionista ou detentor de mais de 5% (cinco por cento) do capital com direito a voto, responsável técnico ou subcontratado, quando a contratação versar sobre obra, serviços ou fornecimento de bens a ela necessários;

c) pessoa física ou jurídica que se encontre, ao tempo da contratação, impossibilitada de contratar em decorrência de sanção que lhe foi imposta;

d) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe 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;

e) empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;

f) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do aviso, tenha sido condenada judicialmente, com trânsito em julgado, por exploração de trabalho infantil, por submissão de trabalhadores a condições análogas às de escravo ou por contratação de adolescentes nos casos vedados pela legislação trabalhista

1.4.3.1. Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico;

1.4.3.2. aplica-se o disposto na alínea “c” também ao fornecedor que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do fornecedor;

1.4.4. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição (Acórdão nº 746/2014-TCU-Plenário).

2. INGRESSO NA DISPENSA ELETRÔNICA E CADASTRAMENTO DA PROPOSTA INICIAL

2.1. O ingresso do fornecedor na disputa da dispensa eletrônica se dará com o cadastramento de sua proposta inicial, na forma deste item.

2.2. O fornecedor interessado, após a divulgação do aviso de contratação direta, encaminhará, exclusivamente por meio do Sistema de Dispensa Eletrônica, a proposta com a descrição do objeto ofertado, a marca do produto, quando for o caso, e o preço, até a data e o horário estabelecidos para abertura do procedimento.

2.2.1. A proposta também deverá conter declaração de que compreende a

integralidade dos custos para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

2.3. Todas as especificações do objeto contidas na proposta, em especial o preço, vinculam a Contratada.

2.4. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na prestação dos serviços;

2.4.1. Os preços ofertados, tanto na proposta inicial, quanto na etapa de lances, serão de exclusiva responsabilidade do fornecedor, não lhe assistindo o direito de pleitear qualquer alteração, sob alegação de erro, omissão ou qualquer outro pretexto.

2.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.

2.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.

2.7. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o *Termo de Referência*, assumindo o proponente o compromisso de executar os serviços nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.

2.8. Uma vez enviada a proposta no sistema, os fornecedores **NÃO** poderão retirá-la, substituí-la ou modificá-la;

2.9. No cadastramento da proposta inicial, o fornecedor deverá, também, assinalar “sim” ou “não” em campo próprio do sistema eletrônico, às seguintes declarações:

2.9.1. que inexistem fatos impeditivos para sua habilitação no certame, ciente da obrigatoriedade de declarar ocorrências posteriores;

2.9.2. que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49.

2.9.3. que está ciente e concorda com as condições contidas no Aviso de Contratação Direta e seus anexos;

2.9.4. que assume a responsabilidade pelas transações que forem efetuadas no sistema, assumindo como firmes e verdadeiras;

2.9.5. que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, de que trata o art. 93 da Lei nº 8.213/91.

2.9.6. que não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do artigo 7°, XXXIII, da Constituição;

2.10. Fica facultado ao fornecedor, ao cadastrar sua proposta inicial, a parametrização de valor final mínimo, com o registro do seu lance final aceitável (menor preço).

2.10.1. Feita essa opção os lances serão enviados automaticamente pelo sistema, respeitados os limites cadastrados pelo fornecedor e o intervalo mínimo entre lances previsto neste aviso.

2.10.1.1. Sem prejuízo do disposto acima, os lances poderão ser enviados

manualmente, na forma da seção respectiva deste Aviso de Contratação Direta;

2.10.2. O valor final mínimo poderá ser alterado pelo fornecedor durante a fase de disputa, desde que não assuma valor superior a lance já registrado por ele no sistema.

2.10.3. O valor mínimo parametrizado possui caráter sigiloso aos demais participantes do certame e para o órgão ou entidade contratante. Apenas os lances efetivamente enviados poderão ser conhecidos dos fornecedores na forma da seção seguinte deste Aviso.

3. FASE DE LANCES

3.1. A partir das 8:00h da data estabelecida neste Aviso de Contratação Direta, a sessão pública será automaticamente aberta pelo sistema para o envio de lances públicos e sucessivos, exclusivamente por meio do sistema eletrônico, sendo encerrado no horário de finalização de lances também já previsto neste aviso.

3.2. Iniciada a etapa competitiva, os fornecedores deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.

3.2.1. O lance deverá ser ofertado pelo valor total do item.

3.3. O fornecedor somente poderá oferecer valor inferior ou maior percentual de desconto em relação ao último lance por ele ofertado e registrado pelo sistema.

3.3.1. O fornecedor poderá oferecer lances sucessivos iguais ou superiores ao lance que esteja vencendo o certame, desde que inferiores ao menor por ele ofertado e registrado pelo sistema, sendo tais lances definidos como “lances intermediários” para os fins deste Aviso de Contratação Direta.

3.3.2. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao que cobrir a melhor oferta é de ***R$1,00 (um real).***

3.4. Havendo lances iguais ao menor já ofertado, prevalecerá aquele que for recebido e registrado primeiro no sistema.

3.5. Caso o fornecedor não apresente lances, concorrerá com o valor de sua proposta.

3.6. Durante o procedimento, os fornecedores serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do fornecedor.

3.7. Imediatamente após o término do prazo estabelecido para a fase de lances, haverá o seu encerramento, com o ordenamento e divulgação dos lances, pelo sistema, em ordem crescente de classificação.

3.7.1. O encerramento da fase de lances ocorrerá de forma automática pontualmente no horário indicado, sem qualquer possibilidade de prorrogação e não havendo tempo aleatório ou mecanismo similar.

4. JULGAMENTO DAS PROPOSTAS DE PREÇO

4.1. Encerrada a fase de lances, será verificada a conformidade da proposta classificada em primeiro lugar quanto à adequação do objeto e à compatibilidade do preço em relação ao estipulado para a contratação.

4.2. No caso de o preço da proposta vencedora estar acima do estimado pela Administração, poderá haver a negociação de condições mais vantajosas.

4.2.1. Neste caso, será encaminhada contraproposta ao fornecedor que tenha apresentado o melhor preço, para que seja obtida melhor proposta com preço compatível ao estimado pela Administração.

4.2.2. A negociação poderá ser feita com os demais fornecedores classificados, respeitada a ordem de classificação, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido para a contratação.

4.2.3. Em qualquer caso, concluída a negociação, o resultado será registrado na ata do procedimento da dispensa eletrônica.

4.3. Estando o preço compatível, será solicitado o envio da proposta e, se necessário, de documentos complementares, adequada ao último lance.

4.4. O prazo de validade da proposta não será inferior a 30 (trinta) dias**,** a contar da data de sua apresentação.

4.5. Será desclassificada a proposta vencedora que:

4.5.1. contiver vícios insanáveis;

4.5.2. não obedecer às especificações técnicas pormenorizadas neste aviso ou em seus anexos;

4.5.3. apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

4.5.4. não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

4.5.5. apresentar desconformidade com quaisquer outras exigências deste aviso ou seus anexos, desde que insanável.

4.6. Quando o fornecedor não conseguir comprovar que possui ou possuirá recursos suficientes para executar a contento o objeto, será considerada inexequível a proposta de preços ou menor lance que:

4.6.1. for insuficiente para a cobertura dos custos da contratação, apresente preços global ou unitários simbólicos, irrisórios ou de valor zero, incompatíveis com os preços dos insumos e salários de mercado, acrescidos dos respectivos encargos, ainda que o ato convocatório da dispensa não tenha estabelecido limites mínimos, exceto quando se referirem a materiais e instalações de propriedade do próprio fornecedor, para os quais ele renuncie a parcela ou à totalidade da remuneração.

4.6.2. apresentar um ou mais valores da planilha de custo que sejam inferiores àqueles fixados em instrumentos de caráter normativo obrigatório, tais como leis, medidas provisórias e convenções coletivas de trabalho vigentes.

4.7. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.

4.8. Erros no preenchimento da planilha não constituem motivo para a desclassificação da proposta. A planilha poderá ser ajustada pelo fornecedor, no prazo indicado pelo sistema, desde que não haja majoração do preço.

4.8.1. O ajuste de que trata este dispositivo se limita a sanar erros ou falhas que não alterem a substância das propostas;

4.8.2. Considera-se erro no preenchimento da planilha passível de correção a indicação de recolhimento de impostos e contribuições na forma do Simples Nacional, quando não cabível esse regime.

4.9. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço

ou da área especializada no objeto.

4.10. Se a proposta ou lance vencedor for desclassificado, será examinada a proposta ou lance subsequente, e, assim sucessivamente, na ordem de classificação.

4.11. Havendo necessidade, a sessão será suspensa, informando-se no “chat” a nova data e horário para a sua continuidade.

4.12. Encerrada a análise quanto à aceitação da proposta, se iniciará a fase de habilitação, observado o disposto neste Aviso de Contratação Direta.

5. HABILITAÇÃO

5.1. Os documentos a serem exigidos para fins de habilitação constam do **ANEXO I – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO** deste aviso e serão solicitados do fornecedor mais bem classificado da fase de lances.

5.2. Como condição prévia ao exame da documentação de habilitação do fornecedor detentor da proposta classificada em primeiro lugar, será verificado o eventual descumprimento das condições de participação, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

b) Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (www.portaldatransparencia.gov.br/ceis);

c) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa, mantido pelo Conselho Nacional de Justiça (www.cnj.jus.br/improbidade_adm/consultar_requerido.php).

d) Lista de Inidôneos mantida pelo Tribunal de Contas da União - TCU;

5.2.1. Para a consulta de fornecedores pessoa jurídica poderá haver a substituição das consultas das alíneas “b”, “c” e “d” acima pela Consulta Consolidada de Pessoa Jurídica do TCU (https://certidoesapf.apps.tcu.gov.br/)

5.2.2. A consulta aos cadastros será realizada em nome da empresa fornecedora e também de seu sócio majoritário, por força do artigo 12 da Lei n° 8.429, de 1992, que prevê, dentre as sanções impostas ao responsável pela prática de ato de improbidade administrativa, a proibição de contratar com o Poder Público, inclusive por intermédio de pessoa jurídica da qual seja sócio majoritário.

5.2.2.1. Caso conste na Consulta de Situação do Fornecedor a existência de Ocorrências Impeditivas Indiretas, o gestor diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas.

5.2.2.1.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros.

5.2.2.1.2. O fornecedor será convocado para manifestação previamente à sua desclassificação

5.2.3. Constatada a existência de sanção, o fornecedor será reputado inabilitado, por falta de condição de participação.

5.3. Caso atendidas as condições de participação, a habilitação dos fornecedores será verificada por meio do SICAF, nos documentos por ele abrangidos.

5.3.1. É dever do fornecedor atualizar previamente as comprovações constantes do SICAF para que estejam vigentes na data da abertura da sessão pública, ou encaminhar, quando solicitado, a respectiva documentação atualizada.

5.3.2. O descumprimento do subitem acima implicará a inabilitação do fornecedor, exceto se a consulta aos sítios eletrônicos oficiais emissores de certidões lograr êxito em encontrar a(s) certidão(ões) válida(s).

5.4. Havendo a necessidade de envio de documentos de habilitação complementares, necessários à confirmação daqueles exigidos neste Aviso de Contratação Direta e já apresentados, o fornecedor será convocado a encaminhá-los, em formato digital, após solicitação da Administração, sob pena de inabilitação.

5.5. Somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não-digitais quando houver dúvida em relação à integridade do documento digital.

5.6. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado (a) da prova de inscrição nos cadastros de contribuintes estadual e municipal e (b) da apresentação do balanço patrimonial e das demonstrações contábeis do último exercício.

5.7. Havendo necessidade de analisar minuciosamente os documentos exigidos, a sessão será suspensa, sendo informada a nova data e horário para a sua continuidade.

5.8. Será inabilitado o fornecedor que não comprovar sua habilitação, seja por não apresentar quaisquer dos documentos exigidos, ou apresentá-los em desacordo com o estabelecido neste Aviso de Contratação Direta.

5.8.1. Na hipótese de o fornecedor não atender às exigências para a habilitação, o órgão ou entidade examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda às especificações do objeto e as condições de habilitação

5.9. Constatado o atendimento às exigências de habilitação, o fornecedor será habilitado

6. CONTRATAÇÃO

6.1. Após a homologação e adjudicação, caso se conclua pela contratação, será firmado Termo de Contrato ou emitido instrumento equivalente.

6.2. O adjudicatário terá o prazo de **02 (dois) dias úteis**, contados a partir da data de sua convocação, para aceitar a autorização de fornecimento, sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Aviso de Contratação Direta.

6.2.1. O prazo previsto para assinatura do contrato ou aceitação da nota de empenho ou instrumento equivalente poderá ser prorrogado 1 (uma) vez, por igual período, por solicitação justificada do adjudicatário e aceita pela Administração.

6.3. O Aceite da Autorização de Fornecimento, emitida à empresa adjudicada, implica no reconhecimento de que:

6.3.1. referida autorização está substituindo o contrato, aplicando-se à relação de negócios ali estabelecida as disposições da Lei nº 14.133, de 2021;

6.3.2. a contratada se vincula à sua proposta e às previsões contidas no Aviso de Contratação Direta e seus anexos;

6.3.3. a contratada reconhece que as hipóteses de rescisão são aquelas previstas nos artigos 137 e 138 da Lei nº 14.133/21 e reconhece os direitos da Administração previstos nos artigos 137 a 139 da mesma Lei.

6.4. O prazo de vigência da contratação é de 30 (TRINTA) DIAS prorrogável conforme previsão nos anexos a este Aviso de Contratação Direta.

6.5. Na assinatura do contrato ou do instrumento equivalente será exigida a comprovação das condições de habilitação e contratação consignadas neste aviso, que deverão ser mantidas pelo fornecedor durante a vigência do contrato.

7. SANÇÕES

7.1. Comete infração administrativa o fornecedor que cometer quaisquer das infrações previstas no art. 155 da Lei nº 14.133, de 2021, quais sejam:

7.1.1. dar causa à inexecução parcial do contrato;

7.1.2. dar causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

7.1.3. dar causa à inexecução total do contrato;

7.1.4. deixar de entregar a documentação exigida para o certame;

7.1.5. não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

7.1.7. ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

7.1.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a dispensa eletrônica ou a execução do contrato;

7.1.9. fraudar a dispensa eletrônica ou praticar ato fraudulento na execução do contrato;

7.1.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

7.1.10.1. Considera-se comportamento inidôneo, entre outros, a declaração falsa quanto às condições de participação, quanto ao enquadramento como ME/EPP ou o conluio entre os fornecedores, em qualquer momento da dispensa, mesmo após o encerramento da fase de lances.

7.1.11. praticar atos ilícitos com vistas a frustrar os objetivos deste certame.

7.1.12. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

7.2. O fornecedor que cometer qualquer das infrações discriminadas nos subitens anteriores ficará sujeito, sem prejuízo da responsabilidade civil e criminal, às seguintes sanções:

a) Advertência pela falta do subitem 8.1.1 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

b) Multa de **10% (dez por cento)** sobre o valor estimado do(s) item(s) prejudicado(s) pela conduta do fornecedor, por qualquer das infrações dos subitens 8.1.1 a 8.1.12;

c) Impedimento de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo que tiver aplicado a sanção, pelo prazo máximo de 3 (três) anos, nos casos dos subitens 8.1.2 a 8.1.7 deste Aviso de Contratação Direta, quando não se justificar a imposição de penalidade mais grave;

d) Declaração de inidoneidade para licitar ou contratar, que impedirá o responsável

de licitar ou contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo mínimo de 3 (três) anos e máximo de 6 (seis) anos, nos casos dos subitens 8.1.8 a 8.1.12, bem como nos demais casos que justifiquem a imposição da penalidade mais grave;

7.3. Na aplicação das sanções serão considerados:

7.3.1. a natureza e a gravidade da infração cometida;

7.3.2. as peculiaridades do caso concreto;

7.3.3. as circunstâncias agravantes ou atenuantes;

7.3.4. os danos que dela provierem para a Administração Pública;

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

7.4. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor de pagamento eventualmente devido pela Administração ao contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente.

7.5. A aplicação das sanções previstas neste Aviso de Contratação Direta, em hipótese alguma, a obrigação de reparação integral do dano causado à Administração Pública.

7.6. A penalidade de multa pode ser aplicada cumulativamente com as demais sanções.

7.7. Se, durante o processo de aplicação de penalidade, houver indícios de prática de infração administrativa tipificada pela Lei nº 12.846, de 1º de agosto de 2013, como ato lesivo à administração pública nacional ou estrangeira, cópias do processo administrativo necessárias à apuração da responsabilidade da empresa deverão ser remetidas à autoridade competente, com despacho fundamentado, para ciência e decisão sobre a eventual instauração de investigação preliminar ou Processo Administrativo de Responsabilização – PAR.

7.8. A apuração e o julgamento das demais infrações administrativas não consideradas como ato lesivo à Administração Pública nacional ou estrangeira nos termos da Lei nº 12.846, de 1º de agosto de 2013, seguirão seu rito normal na unidade administrativa.

7.9. O processamento do PAR não interfere no seguimento regular dos processos administrativos específicos para apuração da ocorrência de danos e prejuízos à Administração Pública Federal resultantes de ato lesivo cometido por pessoa jurídica, com ou sem a participação de agente público.

7.10. A aplicação de qualquer das penalidades previstas realizar-se-á em processo administrativo que assegurará o contraditório e a ampla defesa ao fornecedor/adjudicatário, observando-se o procedimento previsto na Lei nº 14.133, de 2021, e subsidiariamente na Lei nº 9.784, de 1999.

7.11. As sanções por atos praticados no decorrer da contratação estão previstas nos anexos a este Aviso.

8. DAS DISPOSIÇÕES GERAIS

8.1. O procedimento será divulgado no Comprasnet 4.0 e no Portal Nacional de Contratações Públicas - PNCP, e encaminhado automaticamente aos fornecedores registrados no Sistema de Registro Cadastral Unificado - Sicaf, por mensagem eletrônica, na correspondente linha de fornecimento que pretende atender.

8.2. No caso de todos os fornecedores restarem desclassificados ou inabilitados (procedimento fracassado), a Administração poderá:

8.2.1. republicar o presente aviso com uma nova data;

8.2.2. valer-se, para a contratação, de proposta obtida na pesquisa de preços que serviu de base ao procedimento, se houver, privilegiando-se os menores preços, sempre que possível, e desde que atendidas às condições de habilitação exigidas.

8.2.2.1. No caso do subitem anterior, a contratação será operacionalizada fora deste procedimento.

8.2.3. fixar prazo para que possa haver adequação das propostas ou da documentação de habilitação, conforme o caso.

8.3. As providências dos subitens 9.2.1 e 9.2.2 acima poderão ser utilizadas se não houver o comparecimento de quaisquer fornecedores interessados (procedimento deserto)

8.4. Havendo a necessidade de realização de ato de qualquer natureza pelos fornecedores, cujo prazo não conste deste Aviso de Contratação Direta, deverá ser atendido o prazo indicado pelo agente competente da Administração na respectiva notificação.

8.5. Caberá ao fornecedor acompanhar as operações, ficando responsável pelo ônus decorrente da perda do negócio diante da inobservância de quaisquer mensagens emitidas pela Administração ou de sua desconexão.

8.6. Não havendo expediente ou ocorrendo qualquer fato superveniente que impeça a realização do certame na data marcada, a sessão será automaticamente transferida para o primeiro dia útil subsequente, no mesmo horário anteriormente estabelecido, desde que não haja comunicação em contrário.

8.7. Os horários estabelecidos na divulgação deste procedimento e durante o envio de lances observarão o horário de Brasília-DF, inclusive para contagem de tempo e registro no Sistema e na documentação relativa ao procedimento.

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

8.9. As normas disciplinadoras deste Aviso de Contratação Direta serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

8.10. Os fornecedores assumem todos os custos de preparação e apresentação de suas propostas e a Administração não será, em nenhum caso, responsável por esses custos, independentemente da condução ou do resultado do processo de contratação.

8.11. Em caso de divergência entre disposições deste Aviso de Contratação Direta e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Aviso.

8.12. Da sessão pública será divulgada Ata no sistema eletrônico.

8.13. Integram este Aviso de Contratação Direta, para todos os fins e efeitos, os seguintes anexos:

8.13.1. ANEXO I – Documentação exigida para Habilitação;

8.13.2. ANEXO II - Termo de Referência;

8.13.3. ANEXO III – Minuta de Autorização de Compra;

Marcos Antônio Tavares Jácome da Costa Britto

Presidente

ANEXO I – DOCUMENTAÇÃO EXIGIDA PARA HABILITAÇÃO

1 **Habilitação jurídica:**

1.1 no caso de empresário individual, inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

1.2 Em se tratando de Microempreendedor Individual – MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio www.portaldoempreendedor.gov.br;

1.3 No caso de sociedade empresária ou empresa individual de responsabilidade limitada - EIRELI: ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado na Junta Comercial da respectiva sede, acompanhado de documento comprobatório de seus administradores;

1.4 inscrição no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz, no caso de ser o participante sucursal, filial ou agência;

1.5 No caso de sociedade simples: inscrição do ato constitutivo no Registro Civil das Pessoas Jurídicas do local de sua sede, acompanhada de prova da indicação dos seus administradores;

1.6 decreto de autorização, em se tratando de sociedade empresária estrangeira em funcionamento no País;

1.7 Os documentos acima deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

2 **Regularidade fiscal, social e trabalhista:**

2.1 prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

2.2 prova de regularidade fiscal perante a Fazenda Nacional, mediante apresentação de certidão expedida conjuntamente pela Secretaria da Receita Federal do Brasil (RFB) e pela Procuradoria-Geral da Fazenda Nacional (PGFN), referente a todos os créditos tributários federais e à Dívida Ativa da União (DAU) por elas administrados, inclusive aqueles relativos à Seguridade Social, nos termos da Portaria Conjunta nº 1.751, de 02/10/2014, do Secretário da Receita Federal do Brasil e da Procuradora-Geral da Fazenda Nacional.

2.3 prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

2.5 prova de regularidade com a Fazenda *Estadual e/ou Municipal* do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

2.6 caso o fornecedor seja considerado isento dos tributos *estaduais* ***ou*** *municipais* relacionados ao objeto contratual, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei;

3 **Qualificação Econômico-Financeira:**

3.1 certidão negativa de falência expedida pelo distribuidor da sede do fornecedor;

4 Qualificação Técnica

4.1 Comprovação de aptidão para a prestação dos serviços ou entrega de material com características semelhantes ao objeto desta dispensa, ou com o item pertinente, mediante a apresentação de atestado(s) fornecido(s) por pessoas jurídicas de direito público ou privado.

Observação caso haja a condição do artigo 20 da IN 67/2021 será cumprida:

Art. 20. No caso de contratações para entrega imediata, considerada aquela com prazo de entrega de até 30 (trinta) dias da ordem de fornecimento, e nas contratações com valores inferiores a 1/4 (um quarto) do limite para dispensa de licitação para compras em geral e nas contratações de produto para pesquisa e desenvolvimento de que trata a alínea "c" do inciso IV do art. 75 da Lei nº14.133, de 2021, somente será exigida das pessoas jurídicas a comprovação da regularidade fiscal federal, social e trabalhista e, das pessoas físicas, a quitação com a Fazenda Federal.

ANEXO II - Termo de Referência;

CONSELHO REGIONAL DE MEDICINA DO ESTADO DO RIO GRANDE DO NORTE

TERMO DE REFERÊNCIA (TR)

Natal, 30 de janeiro de 2026

Licenças de Antivírus

Este Termo de Referência tem por objetivos:

- Estabelecer normas específicas para a contratação de empresa especializada no fornecimento licenças de software antivírus, destinados a renovação das licenças já existentes no Conselho Regional de Medicina do Rio Grande do Norte – CREMERN.

- As pessoas jurídicas interessadas no objeto deste Termo de Referência, antes de apresentarem suas propostas, deverão analisar atentamente este Termo, dirimindo, oportunamente, todas as dúvidas, de modo a não incorrerem em omissões. Omissões estas que jamais poderão ser alegadas em favor de eventuais pretensões de acréscimos dos preços propostos.

1. OBJETO

O objeto do presente Termo de Referência é a renovação/aquisição de **68**(sessenta e oito) licenças do antivírus Kaspersky Next EDR Foundations Brazilian Edition, incluindo atualizações, garantia e suporte técnico pelo período de **12**(doze) meses para continuar cobrindo com a presente solução a demanda de segurança da informação do CREMERN.

2. JUSTIFICATIVA

2.1. Da contratação:

2.1.1. A presente aquisição visa a renovação de licença de software antivírus para o parque de computadores do CREMERN.

2.2.1. A RENOVAÇÃO das licenças já existentes de software antivírus corporativo, justifica-se pela necessidade de garantir a continuidade de proteção e segurança do ambiente de informática do CREMERN, principalmente considerando a existência e o aumento contínuo de softwares maliciosos como vírus, trojan, spyware, adware, worms e outros malwares.

Uma solução corporativa de antivírus torna-se imprescindível para o bom funcionamento dos computadores e servidores de rede da Instituição. Os antivírus são capazes de prevenir infecções por malwares e de também detectar, capturar e eliminá-los.

Esta renovação é, portanto, indispensável para a segurança dos dados e continuidade das atividades desempenhadas pelos setores do CREMERN.

A licença da atual solução de antivírus adotada pelo CREMERN, Kaspersky Next EDR Foundations Brazilian Edition, que vence no dia **20/03/2026**, sendo necessária a presente aquisição para manter o parque de computadores com proteção atualizada contra as ameaças virtuais mais recentes.

Infelizmente no ano de 2020, uma ameaça denominada *ransomware* tornou-se comum e obteve destaque no noticiário nacional devido ao potencial de estrago, afetando, inclusive, alguns CRMs. A ausência de uma licença válida torna o ambiente eletrônico do CREMERN vulnerável a interrupções e transtornos nos serviços.

3. DA QUALIFICAÇÃO TÉCNICA E JURÍDICA

3.1 Qualificação Técnica:

3.1.1. Comprovação, por meio de documento hábil, de que a empresa possui experiência anterior no fornecimento de itens de características semelhantes;

3.2. Qualificação Jurídica (fiscal, social e trabalhista):

3.2.1. Inscrição no Cadastro Nacional da Pessoa Jurídica (CNPJ);

3.2.2. Inscrição no cadastro de contribuintes estadual e/ou municipal, se houver, relativo ao domicílio ou sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

3.2.3. Comprovação da regularidade perante a Fazenda federal, estadual e/ou municipal do domicílio ou sede do licitante, ou outra equivalente, na forma da lei;

3.2.4. Comprovação da regularidade relativa à Seguridade Social e ao FGTS, que demonstre cumprimento dos encargos sociais instituídos por lei;

3.2.5. Comprovação da regularidade perante a Justiça do Trabalho;

3.2.6. Cumprimento do disposto no inciso XXXIII do art. 7º da Constituição Federal

3.2.7. Contrato Social da empresa.

4. DO OBJETO DA CONTRATAÇÃO

1. Do módulo de proteção:

4.1.1. A solução proposta deverá proteger os sistemas operacionais abaixo:

4.1.1.1. Windows 7
4.1.1.2. Windows 8
4.1.1.3. Windows 8.1
4.1.1.4. Windows 10
4.1.1.5. Windows 11

4.1.2. Servidores

4.1.2.1. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

4.1.3. Servidores de terminal Microsoft

4.1.3.1. Serviços de Área de Trabalho Remota da Microsoft baseados no Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022

4.1.4. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.1.4.1.VMware Workstation 17.0.2 Pro
4.1.4.2.VMware ESXi 8.0 Update 2
4.1.4.3.Microsoft Hyper-V Server 2019
4.1.4.4.Citrix Virtual Apps e Desktop 7 2308
4.1.4.5.Citrix Provisioning 2308
4.1.4.6.Citrix Hypervisor 8.2 Update 1

4.1.5. Sistemas operacionais Linux de 64 bits:

4.1.5.1.Debian GNU/Linux 11.0 e posterior.
4.1.5.2.Debian GNU/Linux 12.0 e posterior.

2. Do módulo de gerenciamento avançado

4.2.1. A solução proposta deve suportar arquitetura cloud-native e on-premisse;

4.2.2. A solução proposta deve incluir suporte para implantação baseada em nuvem por meio de:

4.2.2.1. Amazon Web Services
4.2.2.2.Microsoft Azure

4.2.3. A solução proposta deve fornecer a capacidade de integração com as soluções Managed Endpoint Detection and Response (MDR) e Anti-APT do próprio fornecedor, para caça ativa a ameaças e resposta automatizada a incidentes.

4.2.4. A solução proposta deve ter a capacidade de permitir aplicações baseadas em seus certificados de assinatura digital, MD5, SHA256, metadados, caminho do arquivo e categorias de segurança pré-definidas;

4.2.5. A solução proposta deve suportar Single Sign On (SSO) usando NTLM e Kerberos.

4.2.6. O administrador deve ser capaz de adicionar manualmente novos dispositivos à lista de equipamentos ou editar informações sobre equipamentos já existentes na rede.

4.2.7. A solução proposta deve suportar API OPEN e incluir diretrizes para integração com sistemas externos de terceiros.

4.2.8. A solução proposta deve incluir uma ferramenta integrada para realizar diagnósticos remotos e coletar logs de solução de problemas sem exigir acesso físico ao computador.

4.2.9. A solução proposta deve incorporar no sensor de endpoint distribuição/retransmissão para transferir ou fazer proxy de solicitações de reputação de ameaças dos terminais para o servidor de gerenciamento.

4.2.10. A solução proposta deve suportar o download de arquivos diferenciais em vez de pacotes completos de atualização.

4.2.11. A solução proposta deve incluir Role Based Access Control (RBAC) com funções predefinidas personalizáveis.

4.2.12. O servidor de gerenciamento primário da solução proposta deve ser capaz de retransmitir atualizações e serviços de reputação em nuvem.

4.2.12.1. O servidor de gerenciamento da solução proposta deve ter funcionalidade para criar múltiplos perfis dentro de uma política de proteção com diferentes configurações de proteção que possam estar simultaneamente ativas em uns único/múltiplos dispositivos com base nas seguintes regras de ativação:

4.2.12.2. Status do dispositivo

4.2.12.3. Tag

4.2.12.4. Diretório ativo

4.2.12.5. Proprietários de dispositivos

4.2.12.6. Hardware

4.2.13. A solução proposta deve suportar os seguintes canais de entrega de notificação:

4.2.13.1. E-mail

4.2.13.2. Registro de sistema

4.2.13.3. SMS

4.2.14. A solução proposta deve ter a capacidade de etiquetar/marcar computadores com base em:

4.2.14.1. Atributos de rede

4.2.14.2. Nome

4.2.14.3. Domínio e/ou Sufixo de Domínio

4.2.14.4. Endereço de IP

4.2.14.5. Endereço IP para servidor de gerenciamento

4.2.14.6. Localização no Active Directory

4.2.14.7. Unidade organizacional

4.2.14.8. Grupo

4.2.14.9. Sistema operacional

4.2.14.10. Número do pacote de serviço

4.2.14.11. Arquitetura Virtual

4.2.14.12. Registro de aplicativos

4.2.14.13. Nome da Aplicação

4.2.14.14. Versão do aplicativo

4.2.14.15. Fabricante

4.2.14.16. Tipo e versão

4.2.14.17. Arquitetura

4.2.15. A solução proposta deve ter a capacidade de criar/definir configurações com base na localização de um computador na rede, e não no grupo ao qual pertence no servidor de gestão.

4.2.16. A solução proposta deve ter a funcionalidade de adicionar um mediador de conexão unidirecional entre o servidor de gerenciamento e o endpoint conectado pela internet/rede pública.

4.2.17. As informações sobre o equipamento deverão ser atualizadas após cada nova pesquisa na rede. A lista de equipamentos detectados deve abranger o seguinte:

4.2.17.1. Dispositivos Desktop/Servidores

4.2.17.2. Dispositivos móveis

4.2.17.3. Dispositivos de rede

4.2.17.4. Dispositivos virtuais

4.2.17.5. Componentes OEM

4.2.17.6. Periféricos de computador

4.2.17.7. Dispositivos IoT conectados

4.2.17.8. Telefones VoIP

4.2.17.9. Repositórios de rede

4.2.18. A solução proposta deve permitir ao administrador criar categorias/grupos de aplicação com base em:

4.2.18.1. Nome da Aplicação

4.2.18.2. Caminho do aplicativo

4.2.18.3. Metadados do aplicativo

4.2.18.4. Aplicativo Certificado digital

4.2.18.5. Categorias de aplicativos predefinidas pelo fornecedor

4.2.18.6. SHA256 e MD5

4.2.19. A solução proposta deverá permitir especificamente o bloqueio dos seguintes dispositivos:

4.2.19.1. Bluetooth

4.2.19.2. Dispositivos móveis

4.2.19.3. Modems externos

4.2.19.4. CD/DVD

4.2.19.5. Câmeras e scanners

4.2.19.6. MTPs

4.2.19.7. E a transferência de dados para dispositivos móveis

4.2.20. A solução proposta deve ter capacidade de ler informações do Active Directory para obter dados sobre contas de computadores na organização.

4.2.21. A solução sugerida deve ter funcionalidade integrada para conectar-se remotamente ao endpoint usando a tecnologia Windows Desktop Sharing. Além disso, a solução deve ser capaz de manter a auditoria das ações do administrador durante a sessão.

4.2.22. A solução proposta deverá possuir a funcionalidade de criar uma estrutura de grupos de administração utilizando a hierarquia de Grupos, com base nos seguintes dados:

4.2.22.1. Estruturas de domínios e grupos de trabalho do Windows

4.2.22.2. Estruturas de grupos do Active Directory

4.2.22.3. Conteúdo de um arquivo de texto criado manualmente pelo administrador

4.2.23. A solução proposta deve ser capaz de recuperar informações sobre os equipamentos detectados durante uma pesquisa na rede. O inventário resultante deverá abranger todos os equipamentos conectados à rede da organização.

4.2.24. A solução proposta deve permitir realizar as seguintes ações para endpoints:

4.2.24.1. Verificação manual;

4.2.24.2. Verificação no acesso;

4.2.24.3. Verificação por demanda;

4.2.24.4. Verificação de arquivos compactados

4.2.24.5. Verificação de arquivos individuais, pastas e unidades;

4.2.24.6. Bloqueio e verificação de scripts

4.2.24.7. Proteção contra alteração de registros;

4.2.24.8. Proteção contra estouro de buffer;

4.2.24.9. Verificação em segundo plano/inativa

4.2.25. Verificação de unidade removível na conexão com o sistema;

4.2.26. A solução proposta deve suportar a instalação do sensor de endpoint juntamente com soluções de terceiros, seja utilizando somente o módulo de EDR ou anti-malware.

4.2.27. O servidor de gerenciamento da solução proposta deve manter um histórico de revisões das políticas, tarefas, pacotes, grupos de gerenciamento criados, para que modificações em uma determinada política/tarefa possam ser revisadas.

4.2.28. A solução proposta deve ter a capacidade de definir um intervalo de endereços IP, de forma a limitar o tráfego do cliente para o servidor de gestão com base no tempo e na velocidade.

4.2.29. A solução proposta deve ter a capacidade de realizar inventário em scripts e arquivos, tais como: dll, exe, bat e etc.

4.2.30. A solução proposta deve prever a criação de uma cópia de segurança do sistema de administração com o auxílio de ferramentas integradas do sistema de administração.

4.2.31. A solução proposta deve suportar Windows Failover Cluster.

4.2.32. A solução proposta deve ter um recurso de clustering integrado.

4.2.33. A solução proposta deve incluir alguma forma de sistema para controlar epidemias de vírus.

4.2.34. A solução proposta deve incluir Role Based Access Control (RBAC), e isso deve permitir que as restrições sejam replicadas em todos os servidores de gerenciamento na hierarquia.

4.2.35. O servidor de gestão da solução proposta deverá incluir funções de segurança pré-definidas para o Auditor, Supervisor e Oficial de Segurança.

4.2.36. A solução proposta deve permitir ao administrador criar um túnel de conexão entre um dispositivo cliente remoto e o servidor de gerenciamento caso a porta usada para conexão ao servidor de gerenciamento não esteja disponível no dispositivo.

4.2.37. A solução proposta deve ter a capacidade de priorizar rotinas de varredura personalizadas e sob demanda para estações de trabalho Linux.

4.2.38. A solução proposta deve ser capaz de registrar operações de arquivos (Escrita e Exclusão) em dispositivos de armazenamento USB.

4.2.39. A solução proposta deve ter capacidade de bloquear a execução de qualquer executável do dispositivo de armazenamento USB.

4.2.40. A solução proposta deve contar com filtragem de firewall por endereço local, interface física e Time-To-Live (TTL) de pacotes.

4.2.41. A solução proposta deverá possuir controles para download de DLL e drivers.

4.2.42. A solução proposta deve ter a capacidade de restringir as atividades do aplicativo dentro do sistema de acordo com o nível de confiança atribuído ao aplicativo e de limitar os direitos dos aplicativos de acessar determinados recursos, incluindo arquivos do sistema e do usuário utilizando de módulo especifico de prevenção de intrusão.

4.2.43. A solução proposta deve ter a capacidade de excluir automaticamente as regras de controle de aplicativos se um aplicativo não for iniciado durante um intervalo especificado. O intervalo deve ser configurável.

4.2.44. A solução proposta deve incluir múltiplas formas de notificar o administrador sobre eventos importantes que ocorreram (notificação por e-mail, anúncio sonoro, janela pop-up, entrada de log).

4.2.45. A solução proposta deve incluir Controle de inicialização de aplicativos para o sistema operacional Windows Server.

4.2.46. A solução proposta deve distribuir automaticamente as contas de computador por grupo de gerenciamento caso novos computadores apareçam na rede. Deve fornecer a capacidade de definir as regras de transferência de acordo com o endereço IP, tipo de sistema operacional e localização nas Unidades Organizacionais do Active Directory.

4.2.47. A solução proposta deve permitir o teste de atualizações baixadas por meio do software de administração centralizado antes de distribuí-las às máquinas dos clientes e a entrega das atualizações aos locais de trabalho dos usuários imediatamente após recebê-las.
4.2.48. A solução proposta deve permitir a criação de uma hierarquia de servidores de administração a um nível arbitrário e a capacidade de gerir centralmente toda a hierarquia a partir do nível superior.
4.2.49. A solução proposta deve suportar o Modo de Serviços Gerenciados para servidores de administração, para que instâncias de servidores de administração isoladas logicamente possam ser configuradas para diferentes usuários e grupos de usuários.
4.2.50. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança antimalware através do servidor de administração.
4.2.51. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.
4.2.52. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações antimalware instalados, e para distribuir notificações sobre eventos por e-mail.
4.2.53. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.
4.2.54. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de retransmissão de atualizações e pacotes de instalação, a fim de reduzir a carga da rede no sistema principal do servidor de administração.
4.2.55. A solução proposta deve ter a capacidade de especificar qualquer computador da organização como centro de encaminhamento de eventos do sensor de endpoint do grupo selecionado de computadores clientes para o servidor de administração centralizado, a fim de reduzir a carga da rede no sistema do servidor de administração principal.
4.2.56. A solução proposta deve ser capaz de gerar relatórios gráficos para eventos de software anti-malware e dados sobre inventário de hardware e software, licenciamento, etc.
4.2.57. A solução proposta deve permitir que o administrador defina configurações restritas nas configurações de política/perfil, para que uma tarefa de verificação de vírus possa ser acionada automaticamente quando um determinado número de vírus for detectado durante um período de tempo definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.
4.2.58. A solução proposta deve permitir ao administrador personalizar relatórios.
4.2.59. A solução proposta deve ter a funcionalidade de detectar máquinas virtuais não persistentes e excluí-las automaticamente e seus dados relacionados do servidor de gerenciamento quando desligado.
4.2.60. A solução proposta deve permitir ao administrador definir um período de tempo após o qual um computador não conectado ao servidor de gerenciamento e seus dados relacionados serão automaticamente excluídos do servidor.
4.2.61. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.
4.2.62. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.
4.2.63. A solução proposta deve ter um recurso/módulo integrado para coletar remotamente os dados necessários para solução de problemas dos endpoint, sem exigir acesso físico.
4.2.64. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.
4.2.65. O relatório da solução proposta deve incluir detalhes sobre quais componentes de proteção de endpoint estão ou não instalados em dispositivos clientes, independentemente do perfil de proteção aplicado/existente para esses dispositivos;
4.2.66. O servidor de gerenciamento primário da solução proposta deve ser capaz de recuperar relatórios de informações detalhadas sobre o status de integridade, etc., dos terminais gerenciados dos servidores de gerenciamento secundários.

4.2.67. A solução proposta deve permitir instalar o modulo de gerenciamento on-premisse nos seguintes sistemas operacionais:

4.2.68. Windows

4.2.69. Linux

4.3. A solução proposta deverá suportar os seguintes servidores de banco de dados:

4.3.1. Windows: 4.3.1.1.Microsoft SQL Server

4.3.1.2.Microsoft Banco de dados SQL do Azure

4.3.1.3.MySQL Standard e Enterprise

4.3.1.4.MariaDB

4.3.1.5.PostgreSQL

4.3.2. Linux:

4.3.2.1. MySQL

4.3.2.2. MariaDB

4.3.2.3. PostgreSQL

4.4. A solução proposta deverá suportar as seguintes plataformas virtuais:

4.4.1. Windows:

4.4.1.1. VMware vSphere 6.7 e 7.0

4.4.1.2.Estação de trabalho VMware 16 Pro

4.4.1.3.Servidor Microsoft Hyper-V 2012 de 64 bits

4.4.1.4.Servidor Microsoft Hyper-V 2012 R2 de 64 bits

4.4.1.5.Microsoft Servidor Hyper -V 2016 de 64 bits

4.4.1.6.Servidor Microsoft Hyper-V 2019 de 64 bits

4.4.1.7.Servidor Microsoft Hyper-V 2022 de 64 bits

4.4.1.8.Citrix XenServer 7.1 LTSR

4.4.1.9. Citrix XenServer 8.x

4.4.1.10. Oracle VM VirtualBox 6.x

4.4.2. Linux:

4.4.2.1. VMware vSphere 6.7 e 7.0

4.4.2.2.VMware Desktop 16 Pro e 17 Pro

4.4.2.3.Servidor Microsoft Hyper-V 2012 de 64 bits

4.4.2.4.Servidor Microsoft Hyper-V 2012 R2 de 64 bits

4.4.2.5.Microsoft Servidor Hyper -V 2016 de 64 bits

4.4.2.6.Servidor Microsoft Hyper-V 2019 de 64 bits

4.4.2.7.Servidor Microsoft Hyper-V 2022 de 64 bits

4.4.2.8.Citrix XenServer 7.1 e 8.x

4.4.2.9.Oracle VM VirtualBox 6.x e7.x

5. Do módulo de gerenciamento simplificado

4.5.1. A solução proposta deve suportar arquitetura cloud;

4.5.2. A solução proposta deve incluir um console web integrado para o gerenciamento dos endpoint, que não deve exigir nenhuma instalação adicional.

4.5.3. O console de gerenciamento web da solução proposta deve ser simples de usar e deve suportar dispositivos com tela sensível ao toque.

4.5.4. A solução proposta deve permitir ao administrador gerar relatórios pré-definidos.

4.5.5. A solução proposta deve suportar a descoberta de uso por parte do usuário de aplicações e exibir informações detalhadas de uso de aplicações utilizadas por meios de navegadores e aplicações instaladas no endpoint.

4.5.6. A solução proposta deve atender as condições apontadas no item e subintes 6.

4.5.7. A solução proposta deve suportar sistemas operacionais Windows, Mac, Android e iOS.

4.5.8. A solução proposta deve incluir informações do endpoint:

4.5.8.1. IP público de internet;

4.5.8.2. IP interno do dispositivo;

4.5.8.3.Versão do agente de proteção;

4.5.8.4.Ultima comunicação com a console, contendo data e hora;

4.5.8.5.Informações do sistemas operacional;

6. Requisitos gerais

4.6.1. A solução proposta deve ser capaz de detectar os seguintes tipos de ameaças:

4.6.1.1.Malwares, Worms, Trojans, Backdoors, Rootkits, Spyware, Adware, Ransomware, Keyloggers, Crimeware, sites e links de phishing, vulnerabilidades do tipo ZeroDay e outros softwares maliciosos e indesejados.

4.6.2. A solução proposta deve ser de um único fornecedor e suportar todos módulos descritos neste termo de referência.

4.6.3. A solução proposta deve suportar integração com Anti-malware Scan Interface (AMSI).

4.6.4. A solução proposta deve ter capacidade de integração com a central de segurança do Windows Defender.

4.6.5. A solução proposta deve suportar o subsistema Linux no Windows.

4.6.6. A solução proposta deve fornecer tecnologias de proteção da próxima geração. Sendo no mínimo:

4.6.6.1. Proteção contra ameaças sem arquivos (Fileless);

4.6.6.2. Fornecimento de proteção baseada em machine leaning em várias camadas e análise comportamental durante diferentes estágios da cadeia de ataque;

4.6.7. A solução proposta deve fornecer varredura de memória para estações de trabalho Windows;

4.6.8. A solução proposta deve fornecer varredura de memória do kernel para estações de trabalho Linux.

4.6.9. A solução proposta deve fornecer a capacidade de alternar para o modo nuvem para proteção contra ameaças, diminuindo o uso de RAM e disco rígido em máquinas com recursos limitados.

4.6.10. A solução proposta deve ter componentes dedicados para monitorar, detectar e bloquear atividades em endpoint: Windows, Linux e Mac. Servidores: Windows e Linux, para proteção contra ataques remotos de criptografia.

4.6.11. A solução proposta deve incluir componentes sem assinatura para detectar ameaças mesmo sem atualizações frequentes. A proteção deve ser alimentada por machine learning estático para pré-execução e machine learning dinâmico para estágios pós-execução da cadeia de eliminação em endpoints e na nuvem para servidores e estações de trabalho Windows.

4.6.12. A solução proposta deve fornecer análise comportamental baseada em machine learning.

4.6.13. A solução proposta deve incluir a capacidade de configurar e gerenciar configurações de firewall integradas aos sistemas operacionais Windows Server e Linux, através de seu console de gerenciamento.

4.6.14. A solução proposta deve incluir os seguintes componentes no sensor instalado no endpoint:

4.6.14.1. Controles de aplicativos,

4.6.14.2. Controle web e dispositivos

4.6.14.3. HIPS e Firewall

4.6.14.4. Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;

4.6.15. A capacidade de detectar e bloquear hosts não confiáveis na detecção de atividades semelhantes à criptografia em recursos compartilhados do servidor.

4.6.16. A solução proposta deve ser protegida por senha para evitar que o processo do anti-malware seja interrompido sendo a autoproteção, independentemente do nível de autorização do usuário no sistema.

4.6.17. A solução proposta deve ter bancos de dados de reputação locais e globais.

4.6.18. A solução proposta deve ser capaz de verificar o tráfego HTTPS, HTTP, SMTP e FTP contra malwares.

4.6.19. A solução proposta deve incluir um módulo capaz, no mínimo, de:

4.6.19.1. Bloqueio de aplicativos com base em sua categorização.

4.6.19.2. Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos.

4.6.19.3. A adição de sub-redes e a modificação de permissões de atividade.

4.6.20. A solução proposta deve impedir a conexão de dispositivos USB reprogramados emulando teclados e permitir o controle do uso de teclados na tela mediante autorização.

4.6.21. A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção.

4.6.22. A solução proposta deve ter armazenamento local nos endpoint para manter cópias dos arquivos que foram excluídos ou modificados durante a desinfecção. Esses arquivos devem ser armazenados em um formato específico que garanta que não representem qualquer ameaça.

4.6.23. A solução proposta deve ter uma abordagem proativa para impedir que malware explore vulnerabilidades existentes em servidores e estações de trabalho.

4.6.24. A solução proposta deve suportar a tecnologia AM-PPL (Anti-Malware Protected Process Light) para proteção contra ações maliciosas.

4.6.25. A solução proposta deve incluir proteção contra ataques que explorem vulnerabilidades no protocolo ARP para falsificar o endereço MAC do dispositivo.

4.6.26. A solução proposta deve incluir um componente de controle capaz de aprender a reconhecer o comportamento típico do usuário em um indivíduo ou grupo específico de computadores protegidos e, em seguida, identificar e bloquear ações anômalas e potencialmente prejudiciais realizadas por esse terminal ou usuário.

4.6.27. A solução proposta deve fornecer funcionalidade Anti-Bridging para estações de trabalho Windows para evitar pontes não autorizadas para a rede interna que contornem as ferramentas de proteção de perímetro. Os administradores devem ser capazes de proibir o estabelecimento simultâneo de conexões com fio, Wi-Fi e modem.

4.6.28. A solução proposta deve incluir um componente dedicado para verificação de conexões criptografadas.

4.6.29. A solução proposta deve ser capaz de decriptografar e verificar o tráfego de rede transmitido por conexões criptografadas.

4.6.30. A solução proposta deve ter a capacidade de excluir automaticamente recursos da web quando ocorre um erro de verificação durante a execução de uma verificação de conexão criptografada. Esta exclusão deve ser exclusiva do host e não deve ser compartilhada com outros endpoint;

4.6.31. A solução proposta deve incluir funcionalidade para apagar dados remotamente das estações de trabalho;

4.6.32. A solução proposta deve incluir funcionalidade para excluir automaticamente os dados caso não haja conexão com o servidor de gerenciamento de endpoint.

4.6.33. A solução proposta deve suportar detecção baseadas em multicamadas sendo no mínimo: Assinatura, heurística, machine learning ou assistida por nuvem.

4.6.34. A solução proposta deve ter a capacidade de gerar um alerta, limpar e excluir uma ameaça detectada.

4.6.35. A solução proposta deve ter a capacidade de acelerar as verificações ignorando os objetos que não foram alterados desde a verificação anterior.

4.6.36. A solução proposta deve permitir que o administrador exclua arquivos/pastas/aplicativos/certificados digitais específicos da verificação, seja no acesso (proteção em tempo real) ou durante verificações sob demanda.

4.6.37. A solução proposta deve verificar automaticamente as unidades removíveis em busca de malware quando elas estiverem conectadas a qualquer endpoint.

4.6.38. A solução proposta deve ser capaz de bloquear o uso de dispositivos de

armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

4.6.39. A solução proposta deve ser capaz de diferenciar dispositivos de armazenamento USB, impressoras, celulares e outros periféricos.

4.6.40. A solução proposta deve ter a capacidade de bloquear/permitir o acesso do usuário aos recursos da web com base nos sites e tipo de conteúdo.

4.6.41. A solução proposta deve ter categoria de detecção para bloquear banners de sites.

4.6.42. A solução proposta deve fornecer a capacidade de configurar redes Wi-Fi com base no nome da rede, tipo de autenticação e tipo de criptografia em dispositivos móveis;

4.6.43. A solução proposta deve suportar políticas baseadas no usuário para controle de dispositivos, web e aplicativos.

4.6.44. A solução proposta deve apresentar integração na nuvem, para fornecer atualizações mais rápidas possíveis sobre malware e ameaças potenciais.

4.6.45. A solução proposta deve ter capacidade de gerenciar direitos de acesso de usuários para operações de leitura e gravação em CDs/DVDs, dispositivos de armazenamento removíveis e dispositivos MTP.

4.6.46. A solução proposta deve permitir que o administrador monitore o uso de portas personalizadas/aleatórias pelo aplicativo;

4.6.47. A solução proposta deve suportar o bloqueio de aplicativos proibidos (lista de negações) de serem lançados no endpoint e o bloqueio de todos os aplicativos que não sejam aqueles incluídos nas listas de permissões.

4.6.48. A solução proposta deve ter um componente de controle de aplicativos integrado à nuvem para acesso imediato às atualizações mais recentes sobre classificações e categorias de aplicativos.

4.6.49. A solução proposta deve incluir filtragem de malware de tráfego, verificação de links da web e controle de recursos da web com base em categorias de nuvem.

4.6.50. O componente de controle web da solução proposta deve incluir uma categoria criptomoedas e mineração.

4.6.51. O componente de controle de aplicações da solução proposta deve incluir os modos operacionais lista de negações e lista depermissões.

4.6.52. A solução proposta deve suportar o controle de scripts executados em PowerShell.

4.6.53. A solução proposta deve suportar modo teste com geração de relatórios sobre execução de aplicativos bloqueados.

4.6.54. A solução proposta deve ter a capacidade de controlar o acesso do sistema/aplicativo do usuário a dispositivos de gravação de áudio e vídeo.

4.6.55. A solução proposta deve fornecer um recurso para verificar os aplicativos listados em cada categoria baseada em nuvem.

4.6.56. A solução proposta deve ter capacidade de integração com um sistema avançado de proteção contra ameaças específico do fornecedor.

4.6.57. A solução proposta deve ter a capacidade de regular automaticamente a atividade dos programas em execução, incluindo o acesso ao sistema de arquivos e ao registro, bem como a interação com outros programas.

4.6.58. A solução proposta deve ter a capacidade de categorizar automaticamente os aplicativos iniciados antes da instalação da proteção de endpoint.

4.6.59. A solução proposta deve ter proteção contra ameaças de e-mail de endpoint com:

4.6.59.1. Filtro de anexos.

4.6.59.2. Verificação de mensagens de email ao receber, ler e enviar.

4.6.60. A solução proposta deve ter a capacidade de verificar vários redirecionamentos, URLs encurtados, URLs sequestrados e atrasos baseados em tempo.

4.6.61. A solução proposta deve permitir que o usuário do computador verifique a reputação de um arquivo;

4.6.62. A solução proposta deve incluir a verificação de todos os scripts, incluindo quaisquer scripts WSH (JavaScript, Visual Basic Script Scripts WSH (JavaScript, Visual Basic Script etc.);

4.6.63. A solução proposta deve fornecer proteção contra malware ainda desconhecido com base na análise do seu comportamento e verificação de alterações no registo do

sistema, juntamente com mecanismo de remediação para restaurar automaticamente quaisquer alterações no sistema feitas pelo malware.

4.6.64. A solução proposta deve fornecer proteção contra ataques de hackers por meio de um firewall com sistema de prevenção de intrusões e regras de atividade de rede para aplicações mais populares ao trabalhar em redes de computadores de qualquer tipo, incluindo redes sem fio.

4.6.65. A solução proposta deve incluir suporte ao protocolo IPv6.

4.6.66. A solução proposta deve oferecer a verificação de seções críticas do computador como uma tarefa independente.

4.6.67. A solução proposta deve incorporar a tecnologia de autoproteção de aplicação:

4.6.68. Protegendo contra o gerenciamento remoto não autorizado de um serviço de aplicativo.

4.6.69. Protegendo o acesso aos parâmetros do aplicativo definindo uma senha. Evitando a desativação da proteção por malware, criminosos ou usuários.

4.6.70. A solução proposta deve oferecer a capacidade de escolher quais componentes de proteção contra ameaças instalar.

4.6.71. A solução proposta deve incluir a verificação anti-malware e desinfecção de arquivos em arquivos nos formatos RAR, ARJ, ZIP, CAB, LHA, JAR, ICE, incluindo arquivos protegidos por senha.

4.6.72. A solução proposta deve proteger contra malware ainda desconhecido pertencente a famílias cadastradas, com base em análise heurística.

4.6.73. A solução proposta deve notificar o administrador sobre eventos importantes que ocorreram através de notificação por e-mail.

4.6.74. A solução proposta deve permitir ao administrador criar um único pacote de instalação do sensor de proteção com a configuração necessária.

4.6.75. A solução proposta deve fornecer controles de aplicativos e dispositivos para estações de trabalho Windows.

4.6.76. A proteção da solução proposta para servidores e estações de trabalho deve incluir um componente dedicado para proteção contra atividades de ransomware/malwares que criptografa os recursos compartilhados.

4.6.77. A solução proposta deve, ao detectar atividades semelhantes a ransomware/criptografia , bloquear automaticamente o computador atacante por um intervalo especificado e listar informações sobre o IP e carimbo de data/hora do computador atacante e o tipo de ameaça.

4.6.78. A solução proposta deve fornecer uma lista predefinida de exclusões de verificação para aplicativos e serviços Microsoft.

4.6.79. A solução proposta deve suportar a instalação de proteção de endpoint em servidores sem a necessidade de reinicialização.

4.6.80. A solução proposta deve permitir a instalação de software com funcionalidades de anti-malware e detecção e resposta de incidente a partir de um único pacote de distribuição.

4.6.81. A solução proposta deve suportar endereços IPv6.

4.6.82. A solução proposta deve suportar verificação em duas etapas (autenticação).

4.6.83. A solução proposta deve prever a instalação, atualização e remoção centralizada de software antimalware, juntamente com configuração, administração centralizada e visualização de relatórios e informações estatísticas sobre o seu funcionamento.

4.6.84. A solução proposta deverá contar com a remoção centralizada (manual e automática) de aplicações incompatíveis do centro de administração.

4.6.85. A solução proposta deve fornecer métodos flexíveis para instalação do sensor de endpoint via: RPC, GPO e um agente de administração para instalação remota e a opção de criar um pacote de instalação independente para instalação do endpoint de segurança localmente.

4.6.86. A solução proposta deve permitir a instalação remota do sensor de endpoint com os bancos de dados anti-malware mais recentes.

4.6.87. A solução proposta deve permitir a atualização automática do sensor de endpoint e

de bases de dados de anti-malware.

4.6.88. A solução proposta deve contar com recursos de busca automática de vulnerabilidades em aplicações e no sistema operacional em máquinas protegidas.

4.6.89. A solução proposta deve permitir a gestão de um componente que proíba a instalação e/ou execução de programas.

4.6.90. A solução proposta deve permitir a gestão de um componente que controla o trabalho com dispositivos de E/S externos.

4.6.91. A solução proposta deve permitir o gerenciamento de componente que controle a atividade do usuário na internet.

4.6.92. A solução proposta deve ser capaz de implantar automaticamente proteção para infraestruturas virtuais baseadas em VMware ESXi , Microsoft Hyper-V, plataforma de virtualização Citrix XenServer ou hipervisor.

4.6.93. A solução proposta deve incluir a distribuição automática de licenças nos computadores clientes.

4.6.94. A solução proposta deverá ser capaz de exportar relatórios para arquivos PDF, CSV ou XLS.

4.6.95. A solução proposta deve proporcionar a administração centralizada de armazenamentos de backup e quarentenar em todos os recursos da rede onde o sensor de endpoint está instalado.

4.6.96. A solução proposta deve prever a criação de contas internas para autenticar administradores no servidor de administração.

4.6.97. A solução proposta deverá ter capacidade de gerenciar dispositivos móveis através de comandos remotos.

4.6.98. A solução proposta deve ter a capacidade de excluir atualizações baixadas.

4.6.99. A solução proposta deve mostrar claramente informações sobre a distribuição de vulnerabilidades entre computadores gerenciados.

4.6.100. A interface do servidor de gerenciamento da solução proposta deverá suportar o idioma Inglês e português.

4.6.101. A solução proposta deve ter um painel customizável gerando e exibindo estatísticas em tempo real dos sensores de endpoints.

4.6.102. A solução proposta deve incorporar funcionalidade de distribuição/retransmissão para suportar a entrega de proteção, atualizações, patches e pacotes de instalação para locais e remotos.

4.6.103. Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a tecnologia que a detectou.

4.6.104. A solução proposta deve incluir a opção para implantar uma console de gerenciamento local ou usar o console de gerenciamento baseado em nuvem fornecido pelo fornecedor.

4.6.105. A solução proposta deve ser capaz de se integrar ao console de gerenciamento baseado em nuvem do fornecedor para gerenciamento de endpoint sem custo adicional.

4.6.106. A solução proposta deve permitir a migração rápida do console de gerenciamento local para o console de gerenciamento baseado em nuvem do fornecedor.

4.6.107. A solução proposta deve fornecer mecanismos de atualização de banco de dados, incluindo:

4.6.107.1. Múltiplas formas de atualização, incluindo canais de comunicação globais através do protocolo HTTPS, recursos compartilhados em rede local e mídia removível.

4.6.107.2. Verificação da integridade e autenticidade das atualizações por meio de assinatura digital eletrônica.

4.6.108. A solução proposta deve permitir monitorar vulnerabilidades existentes em dispositivos gerenciados.

4.6.109. A solução proposta deve gerar relatoiros de vulnerabilidades encontradas nos dispositivos com sensor de end point instalado.

7. Do modulo de gerenciamento de dispositivos móveis

4.7.1. O modulo deve ser integrado a console de gerenciamento;

4.7.2. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android:

4.7.2.1. Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition)

4.7.3. A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS:

7.3.1.iOS 10–17 ou iPadOS 13–17

4.7.4. A solução proposta deve oferecer suporte a dispositivos Android Device Owner.

4.7.5. A solução proposta deve suportar dispositivos iOS supervisionados.

4.7.6. A solução proposta deve permitir a proteção do sistema de arquivos do smartphone e a interceptação e varredura de todos os objetos recebidos transferidos através de conexões sem fio (porta infravermelha, Bluetooth), EMS e MMS, ao mesmo tempo em que sincroniza com o computador pessoal e carrega arquivos através de um navegador.

4.7.7. A solução proposta deve ter a capacidade de bloquear sites maliciosos projetados para espalhar códigos maliciosos e sites de phishing projetados para roubar dados confidenciais do usuário e acessar suas informações financeiras.

4.7.8. A solução proposta deve ter a funcionalidade de adicionar um site excluído da verificação a uma lista de permissões.

4.7.9. A solução proposta deve incluir a filtragem de websites por categorias e permitir ao administrador restringir o acesso dos utilizadores a categorias específicas (por exemplo, websites relacionados com jogos de azar ou categorias de redes sociais).

4.7.10. A solução proposta deve permitir ao administrador obter informações sobre o funcionamento do sensor de endpoint e da proteção web no dispositivo móvel do usuário.

4.7.11. A solução proposta deverá ter a funcionalidade de detectar a localização do dispositivo móvel via GPS, e mostrá-la no Google Maps.

4.7.12. A solução proposta deve permitir ao administrador tirar uma foto da câmera frontal do celular quando ele estiver bloqueado.

4.7.13. A solução proposta deve ter recursos de conteinerização para dispositivos Android.

4.7.14. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos Android:

4.7.14.1. Dados em contêineres

4.7.14.2. Contas de e-mail corporativo

4.7.14.3. Configurações para conexão à rede Wi-Fi corporativa e VPN

4.7.14.4. Nome do ponto de acesso (APN)

4.7.14.5. Perfil do Android for Work

4.7.14.6. Recipiente KNOX

4.7.14.7. Chave do gerenciador de licença KNOX

4.7.15. A solução proposta deve ter a funcionalidade de limpar remotamente o seguinte dos dispositivos iOS:

4.7.15.1. Todos os perfis de configuração instalados

4.7.15.2. Todos os perfis de provisionamento

4.7.15.3. O perfil iOS MDM

4.7.16. Aplicativos para os quais a caixa de seleção remover e o perfil iOS MDM foram marcadas

4.7.17. A solução proposta deve permitir a criptografia de todos os dados do dispositivo (incluindo dados de contas de usuários, unidades removíveis e aplicativos, bem como mensagens de e-mail, mensagens SMS, contatos, fotos e outros arquivos). O acesso aos dados criptografados só deve ser possível em um dispositivo desbloqueado por meio de uma chave especial ou senha de desbloqueio do dispositivo .

4.7.18. A solução proposta deve oferecer controles para garantir que todos os dispositivos cumpram os requisitos de segurança corporativa. O controlo de conformidade deverá basear-se num conjunto de regras que deverá incluir as seguintes componentes:

4.7.18.1. Critérios de verificação do dispositivo;

4.7.18.2. Prazo alocado para o usuário corrigir a não conformidade configurando ação que será tomada no dispositivo caso o usuário não corrija a não conformidade dentro do prazo definido;

4.7.19. A solução proposta deve ter a funcionalidade de detectar e notificar o administrador sobre hacks de dispositivos, por exemplo, root, Jailbreak e etc.

4.7.20. A solução proposta deverá permitir a gestão de pelo menos as seguintes características do dispositivo:

4.7.20.1. Cartões de memória e outras unidades removíveis

4.7.20.2. Câmera do dispositivo

4.7.20.3. Conexões Wi-Fi

4.7.20.4. Conexões Bluetooth

4.7.20.5. Porta de conexão infravermelha

4.7.20.6. Ativação do ponto de acesso Wi-Fi

4.7.20.7. Conexão de área de trabalho remota

4.7.20.8. Sincronização de área de trabalho

4.7.20.9. Definir configurações da caixa de correio do Exchange

4.7.20.10. Configurar caixa de e-mail em dispositivos iOS MDM

4.7.20.11. Configure contêineres Samsung KNOX.

4.7.20.12. Definir as configurações do perfil do Android for Work

4.7.20.13. Configurar e-mail/calendário/contatos

4.7.20.14. Defina as configurações de restrição de conteúdo de mídia.

4.7.20.15. Definir configurações de proxy no dispositivo móvel

4.7.20.16. Configurar certificados e SCEP

4.7.21. A solução proposta deverá permitir a configuração de uma conexão com dispositivos AirPlay para permitir o streaming de músicas, fotos e vídeos do dispositivo iOS MDM para dispositivos AirPlay .

4.7.22. A solução proposta deve suportar todos os métodos de implantação abaixo para o sensor móvel:

4.7.22.1. Portal de inscrição móvel KNOX

4.7.22.2. Pacotes de instalação pré-configurados independentes

4.7.23. A solução proposta deverá permitir a configuração de Nomes de Pontos de Acesso (APN) para conectar um dispositivo móvel a serviços de transferência de dados em uma rede móvel.

4.7.24. A solução proposta deve permitir que o PIN de um dispositivo móvel seja redefinido remotamente.

4.7.25. A solução proposta deve incluir a opção de registrar dispositivos Android usando sistemas EMM de terceiros:

4.7.25.1. VMware AirWatch 9.3 ou posterior

4.7.25.2. MobileIron 10.0 ou posterior

4.7.25.3. IBM MaaS360 10.68 ou posterior

4.7.25.4. Microsoft Intune 1908 ou posterior

4.7.25.5. SOTI MobiControl 14.1.4 (1693) ou posterior

4.7.26. A solução proposta deve ter funcionalidade para forçar a instalação de um aplicativo no dispositivo.

4.7.27. A solução proposta deve ser capaz de escanear arquivos abertos no dispositivo.

4.7.28. A solução proposta deve ser capaz de verificar programas instalados a partir da interface do dispositivo.

4.7.29. A solução proposta deve ser capaz de verificar objetos do sistema de arquivos no dispositivo ou em placas de extensão de memória conectadas, mediante solicitação do usuário ou de acordo com um agendamento.

4.7.30. A solução proposta deve proporcionar o isolamento confiável de objetos infectados em um local de armazenamento de quarentena.

4.7.31. A solução proposta deve contar com a atualização dos bancos de dados de antivírus utilizados para busca de programas maliciosos e exclusão de objetos perigosos.
4.7.32. A solução proposta deve ser capaz de verificar dispositivos móveis em busca de malware e outros objetos indesejados sob demanda e dentro do cronograma e lidar com eles automaticamente.
4.7.33. A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a partir do mesmo console usado para gerenciar computadores e servidores.
4.7.34. A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.
4.7.35. A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.
4.7.36. A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.
4.7.37. A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.
4.7.38. A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.
4.7.39. A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;
4.7.40. A solução proposta deve proteger contra ameaças online em dispositivos iOS.

8. Do módulo de EDR

4.8.1. Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.
4.8.2. Todas as detecções são destacadas no gráfico, fornecendo ao analista o contexto completo para o incidente e facilitando o processo de revelação dos componentes afetados.
4.8.3. A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um gráfico visualizado da cadeia de desenvolvimento de ameaças;
4.8.4. Deve apresentar as seguintes informações:
4.8.4.1.Processo;
4.8.4.2.Arquivos;
4.8.4.3.Chaves de registros;
4.8.4.4.Conexões de rede;
4.8.4.5.SHA256 e MD5;
4.8.5. Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise;
4.8.6. Deve apresentar informações detalhadas contendo:
4.8.6.1.Usuário que executou a ação;
4.8.6.2.Informações acesso privilegiado;

9. Requisitos para documentação da solução.

4.9.1. A documentação da solução do anti-malware incluindo ferramentas de administração, deve incluir os seguintes documentos:
4.9.2. Ajuda on-line para administradores
4.9.3. Ajuda on-line para melhores práticas de implementação
4.9.4. Ajuda on-line para proteção de servidores de administração
4.9.5. A documentação do software anti-malware fornecida deve descrever detalhadamente os processos de instalação, configuração e uso do software anti-malware.
4.9.6. Deve estar disponível página com informações de ciclo de vida das soluções e módulos.

5. DAS OBRIGAÇÕES DA CONTRATADA

5.1 São obrigações da empresa CONTRATADA:

5.1.1 Observar e cumprir todas as especificações constantes neste Termo de Referência;

5.1.2 Fornecer os produtos contratados, mediante apresentação da Ordem de Compra emitida pelo Setor de Compras, no prazo máximo de até 15 (quinze) dias corridos, a partir do recebimento do documento;

5.1.3 Responsabilizar-se pela entrega do quantitativo solicitado na sede da CONTRATANTE, situada na Avenida Rio Branco, 398, Cidade Alta, Natal/RN, ressaltando que todas as despesas de transporte e outras necessárias ao cumprimento de suas obrigações serão de responsabilidade da CONTRATADA;

5.1.4 O Fornecimento se dará por meio de documento em duas vias, uma das quais será devolvida com recibo do servidor responsável pelo recebimento e servirá de subsídio para emissão da Nota Fiscal;

5.1.5 Arcar com todas as despesas decorrentes do fornecimento do objeto do presente Termo de Referência, tais como impostos, frete, taxas, seguros, materiais incidentes, enfim, tudo que for necessário ao fornecimento e entrega do produto ao CREMERN;

5.1.6 Responsabilizar-se por todas as despesas diretas ou indiretas, tais como: salários, transportes, encargos sociais, fiscais, trabalhistas, previdenciários e de ordem de classe, indenizações e quaisquer outras que forem devidas aos seus empregados no desempenho dos serviços objeto do contrato, ficando a CONTRATANTE isenta de qualquer vínculo empregatício com os mesmos;

5.1.7 Responsabilizar-se por quaisquer danos pessoais ou materiais causados por seus empregados e acidentes causados a terceiros, bem como pelo pagamento de salários, encargos sociais e trabalhistas, tributos e demais despesas eventuais, decorrentes do objeto deste contrato e mais as constantes da Proposta;

5.1.8 Manter-se, durante toda a execução do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para a habilitação, ou para a qualificação, na contratação direta, exigidas no Termo de Referência, consoante o que preceitua o inciso XVI do artigo 92, da Lei nº. 14.133/2021;

5.1.9 Abster-se de quaisquer iniciativas que impliquem em ônus para o Conselho Regional de Medicina do Rio Grande do Norte – CREMERN, se não previstos neste Termo de Referência e expressamente autorizados pelo CREMERN;

5.1.10 O retardamento na entrega do objeto/execução dos serviços, não justificado considerar-se-á como infração contratual;

5.1.11 Manter com a CONTRATANTE relação sempre formal, por escrito, ressalvados os entendimentos verbais motivados pela urgência, que deverão ser de imediato, confirmados

por escrito;

5.1.12 Apresentar juntamente com a nota fiscal referente à prestação dos serviços, Certidão Negativa de Débito de INSS, FGTS, Certidão de regularidade fiscal perante a Fazenda Federal e Dívida Ativa da União, Estadual e Municipal.

6. DAS OBRIGAÇÕES DA CONTRATANTE

6.1 Constituem obrigações da CONTRATANTE:

6.1.1. Prestar todas as informações e orientações à empresa com relação ao produto a ser ofertado;

6.1.2. Efetuar o pagamento devido nas condições de preço e prazo estabelecidos neste Termo de Referência;

6.1.3. Notificar, por escrito, à CONTRATADA qualquer irregularidade constatada na entrega do objeto;

6.1.4. Comunicar por escrito à CONTRATADA o não recebimento do objeto/não prestação do serviço, apontando as razões de sua não adequação aos termos contratuais;

6.1.5. Receber e fiscalizar a entrega do objeto, verificando sua correspondência com as especificações previstas neste Termo de Referência, atestando sua conformidade;

6.1.6. Rejeitar, no todo ou em parte, o produto entregue em desacordo com as especificações descritas neste Termo de Referência, e com as obrigações assumidas pelo fornecedor;

6.1.7. Facilitar por todos os meios ao cumprimento da execução pela CONTRATADA, dando- lhe acesso e promovendo o bom entendimento entre seus funcionários e empregados da contratada, cumprindo com as obrigações preestabelecidas;

6.1.8. Atestar a Nota Fiscal, por intermédio do gestor, após verificação se a mesma é destinada a Instituição e se corresponde à execução dos serviços prestados;

6.1.9. À CONTRATANTE, é reservado o direito de, sem que de qualquer forma restrinja a plenitude dessa responsabilidade, exercer a mais ampla e completa fiscalização sobre o cumprimento das especificações e condições deste objeto.

7. DAS CONDIÇÕES DO PAGAMENTO

7.1. O pagamento será efetuado em favor da CONTRATADA, mediante apresentação respectiva Nota Fiscal e somente após o recebimento definitivo do objeto, nos termos do art. 140, inciso II, da Lei nº 14.133/2021, e regular liquidação, através de transferência bancária.

7.2. A Nota Fiscal ou Fatura deverá, necessariamente, ser apresentada com os elementos

essenciais do documento, tais como:

a) descrição dos itens fornecidos;

b) o prazo de validade;

c) a data da emissão;

d) os dados do contrato e do órgão contratante;

e) o valor a pagar; e,

f) eventual destaque do valor de retenções tributáveis cabíveis.

7.3. A CONTRATADA deverá apresentar, juntamente com a Nota Fiscal, as seguintes certidões: Certidão Negativa de Débitos relativos a Tributos Federais e Dívida Ativa da União, Certidão Negativa de Débitos relativos as contribuições previdenciárias – CND, Certificado de Regularidade do FGTS – CRF e Certidão Negativa de Débitos Trabalhistas – CNDT.

7.4. Caso a CONTRATADA goze de algum benefício fiscal, esta ficará responsável pela apresentação de documentação hábil, ou, no caso de optante pelo SIMPLES NACIONAL (Lei Complementar nº 123/2006), pela entrega de declaração, conforme modelo constante da IN nº 480/04, alterada pela IN nº 706/07, ambas da Secretaria da Receita Federal. Após apresentada a referida comprovação, a CONTRATADA ficará responsável por comunicar ao CREMERN qualquer alteração posterior na situação declarada, a qualquer tempo, durante a execução do contrato.

7.5. Todas as despesas deverão estar inclusas no preço preposto, e em hipótese alguma poderão ser destacadas quando da emissão da Nota Fiscal/Fatura.

7.6. Quando houver erro, de qualquer natureza, na emissão da Nota Fiscal/Fatura, ou ainda, circunstância que impeça a liquidação da despesa, o pagamento ficará pendente até que sejam providenciadas as medidas saneadoras. Nessa hipótese, o prazo para pagamento iniciar-se-á após a regularização da situação, não acarretando nenhum ônus ao CONTRATANTE.

7.7. Se, por qualquer motivo alheio à vontade do CONTRATANTE, houver atraso na entrega dos bens, o período correspondente não gerará obrigação de pagamento.

7.8. A CONTRATADA deverá arcar com o recolhimento de todos os tributos e contribuições federais, estaduais e municipais, devidos em decorrência do objeto do contrato, inclusive aqueles retidos pelo CREMERN na forma da lei, devendo destacar as retenções tributárias devidas em suas Notas Fiscais, ou entregar documentação comprobatória que comprove a não necessidade de retenção do(s) tributo(s).

7.9. Caso a CONTRATANTE não cumpra o prazo estipulado no item 7.1 pagará à CONTRATADA atualização financeira de acordo com a variação do IPCA/IBGE, proporcionalmente aos dias de atraso.

7.10. Não caberá pagamento de atualização financeira à CONTRATADA caso o pagamento não ocorra no prazo previsto por culpa exclusiva desta.

7.11. No caso de pendência de liquidação de obrigações pela CONTRATADA, em virtude de penalidades impostas, a CONTRATANTE poderá descontar da fatura devida, ou ainda, quando for o caso, cobrada judicialmente.

7.12. Após escolha da CONTRATADA, não será levada em conta qualquer reclamação ou solicitação, seja a que título for, de alteração dos preços constantes da proposta da CONTRATADA.

8. DO INSTRUMENTO CONTRATUAL, DO PRAZO DE FORNECIMENTO E ENTREGA

8.1 A contratação do objeto descrito neste Termo de Referência se dará através de Autorização de Compra, conforme disposição dos incisos II, do art. 95, da Lei nº 14.133/2021, por se tratar de compra com entrega imediata e integral dos bens.

8.2. O fornecimento dos bens se dará de forma imediata e integral, assim considerado o prazo de entrega de até 30 (trinta) dias a contar da data de emissão da Autorização de Compra.

8.3. À Autorização de Compra aplica-se, no que couber, as cláusulas contratuais previstas no art. 92, da Lei nº 14.133/2021.

8.4 Os equipamentos serão entregues na sede do Conselho Regional de Medicina do Rio Grande do Norte – CREMERN (Avenida Rio Branco 398, Cidade Alta- Natal-RN) conforme distribuição no item 4.1.

9. DA FISCALIZAÇÃO DO CONTRATO

9.1. A fiscalização da execução da contratação se dará por meio do fiscal formalmente designado pela autoridade máxima do CREMERN, que anotará em registro próprio todas as ocorrências relacionadas com a execução, determinando o que for necessário à regularização das faltas ou defeitos, observados os ditames da Lei nº 14.133/2021 sobre o assunto.

9.2. Caberá à fiscalização o recebimento provisório do objeto contratual, devendo adotar as providências descritas na alínea “a” do inciso II, do atr. 140 da Lei nº 14.133/2021

9.3. Caberá à Coordenação de Administração do CREMERN o recebimento definitivo do objeto contratual, conforme alínea “b” do inciso II, do atr. 140 da Lei nº 14.133/2021, mediante termo detalhado que comprove o atendimento das exigências contratuais, o qual será encaminhado à fiscalização para conhecimento e atestação da nota fiscal ou fatura apresentada pela CONTRATADA, para fins de liquidação e pagamento.

9.4. A fiscalização de que trata esta cláusula não exclui nem reduz a responsabilidade da CONTRATADA pelos danos causados ao CONTRATANTE ou a terceiros, resultantes de ação ou omissão culposa ou dolosa de quaisquer de seus empregados ou prepostos;

9.5. O fiscal do contrato ficará responsável, ainda, pelo acompanhamento da fiel execução das cláusulas contratuais, bem como pela instrução e eventuais processos de aplicação de penalidades, nos casos de inadimplemento contratual.

10. DA PUBLICIDADE E DA EFICÁCIA DA CONTRATAÇÃO

10.1 A Autorização de Compra será juntada ao processo que tiver dado origem à contratação, divulgada e mantida à disposição do público em sítio eletrônico oficial, conforme art. 91, caput, da Lei nº 14.133/2021.

10.2. A eficácia da Autorização de Compra ficará condicionada à divulgação no Portal Nacional de Contratações Públicas (PNCP) e deverá ocorrer em até 10 (dez) dias úteis a contar da data de sua assinatura, conforme disposição do art. 94, caput e inciso II, da Lei nº 14.133/2021.

11. DA DOTAÇÃO ORÇAMENTÁRIA

11.1 As despesas decorrentes da presente contratação correrão por conta de créditos orçamentários consignados no Orçamento da CONTRATANTE no exercício de 2026 e serão alocados pelo Departamento Financeiro e Contábil deste Conselho.

12. DAS PENALIDADES

12.1. A CONTRATADA deverá observar rigorosamente as condições estabelecidas para a prestação dos serviços, sujeitando-se, no caso de ocorrência de infrações previstas no art. 155 da Lei nº 14.133/2021, as penalidades constantes no art. 156 da Lei nº 14.133/2021, a saber:

12.1.1. Advertência, nos casos de inexecução parcial do contrato;

12.1.2. Multa de 10% (dez por cento) incidente sobre o valor global da contratação, por qualquer das infrações administrativas previstas no art. 155 da Lei nº 14.133/2021;

12.1.3. Impedimento de licitar e contratar; nos casos em que a CONTRATADA:

a) der causa à inexecução parcial do contrato que cause grave dano à Administração, ao funcionamento dos serviços públicos ou ao interesse coletivo;

b) der causa à inexecução total do contrato;

c) deixar de entregar a documentação exigida para o certame;

d) não mantiver a proposta, salvo em decorrência de fato superveniente devidamente justificado;

e) não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

f) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado.

12.1.4. Declaração de inidoneidade para licitar ou contratar:

a) apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação ou a execução do contrato;

b) fraudar a licitação ou praticar ato fraudulento na execução do contrato;

c) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;

d) praticar atos ilícitos com vistas a frustrar os objetivos da licitação;

12.1.5. praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.A aplicação das sanções será precedida de todos os ditames e procedimentos constantes no Título IV da Lei nº 14.133/2021.

13. DOS CASOS OMISSOS E DO FORO

13.1 Fica eleito o Foro da Justiça Federal, Natal- RN, como competente para dirimir quaisquer dúvidas ou ações oriundas do futuro Contrato, com renúncia de qualquer outro por mais privilegiado que seja.

13.2 Os casos omissos serão analisados pelos representantes legais das partes, com o intuito de solucionar o impasse, sem que haja prejuízo para nenhuma delas, tendo por base o que dispõe a Lei n.º 14.133/2021 e demais legislações aplicáveis de forma subsidiária à referida lei.

Luiz Cláudio Carvalho da

Silva Analista de TI do

CREMERN

Documento assinado eletronicamente por **Luiz Claudio Carvalho da Silva**, **Analista de Tecnologia da Informação**, em 30/01/2026, às 11:40, com fundamento no art. 5º da RESOLUÇÃO CFM nº2.308/2022, de 28 de março de 2022.

A autenticidade do documento pode ser conferida no site

Av. Rio Branco, 398 - Bairro Cidade Alta
CEP 59025-001 | Natal/RN -
http://www.cremern.org.br/

MINUTA DE AUTORIZAÇÃO DE COMPRA

Processo Administrativo nº 26.20.00000447-7

Interessado: XXXXXXXXXXXXX - CNPJ: XXXXXXXXXXXXX

Objeto: Renovação/Aquisição de **68**(sessenta e oito) licenças do antivírus Kaspersky Next EDR Fourdations Brazilian Edition, incluindo atualizações, garantia e suporte técnico pelo período de **12**(doze) meses **Justificativa:** A presente aquisição visa a renovação de licença de software antivírus para o parque de computadores do CREMERN.

A RENOVAÇÃO das licenças já existentes de software antivírus corporativo, justifica-se pela necessidade de garantir a continuidade de proteção e segurança do ambiente de informática do CREMERN, principalmente considerando a existência e o aumento contínuo de softwares maliciosos como vírus, trojan, spyware, adware, worms e outros malwares.

Fundamentação Legal: A presente autorização fundamenta-se na Lei nº 14.133/2021, em especial no disposto no artigo 95, que disciplina as contratações públicas. Obedecendo o previsto no Termo de Referência/SEI – Nº 3665893

Valor da Compra: R$ XXXXXXXX

Dotação Orçamentária:

Elemento de Despesa: 6.2.2.1.1.33.90.39.010 – MANUT. DE SISTEMAS DE INFORMÁTICA - SOFTWARE

Responsável pela Autorização: MARCOS ANTONIO T. JÁCOME DA COSTA BRITTO – PRESIDENTE DO CREMERN

Local e Data: Natal/RN – XXXXXXXX

MARCOS ANTONIO T. JÁCOME DA COSTA BRITTO
PRESIDENTE DO CREMERN