EDITAL

PREGÃO ELETRÔNICO Nº 005/2025

(Processo SEI Nº 24.0.000044917-9)

A Assembleia Legislativa do Estado de Santa Catarina – Alesc – CNPJ nº 83.599.191/0001-87, com sede na Rua Doutor Jorge Luz Fontes, nº 310 – Centro – Florianópolis/SC, CEP 88020-900, por meio de sua Coordenadoria de Licitações e Contratos, torna público que realizará, na forma da Lei nº 14.133/2021, da Lei Complementar nº 123/2006 e de outras normas aplicáveis ao objeto deste certame, licitação, na modalidade **PREGÃO ELETRÔNICO,** critério de julgamento **MENOR PREÇO,** mediante as condições estabelecidas neste Edital e em seus Anexos.

DATA DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

DIA: 03/07/2025
ABERTURA DA SESSÃO: 14h
ENDEREÇO ELETRÔNICO: www.compras.gov.br
Nº DA UNIDADE COMPRADORA: 929488
Nº DA COMPRA: 90005/2025
CRITÉRIO DE JULGAMENTO: menor preço
MODO DE DISPUTA: aberto

FUNDAMENTO LEGAL

· Lei Federal nº 14.133, de 1º de abril de 2021;
· Lei Complementar nº 123, de 14 de dezembro de 2006;
· Atos da Mesa nº 149, de 30 de abril de 2020, nº 195, de 16 de junho de 2020, e nº 257, de 28 de maio de 2024;
· Autorização para Processo Licitatório – Despacho SEI Nº 1669255; e
· Processo SEI N° 24.0.000044917-9.

DOS ANEXOS QUE INTEGRAM O EDITAL

Anexo	I	Termo de Referência;
Anexo	II	Planilha de Valores Máximos Admissíveis;
Anexo	III	Modelo de Proposta;
Anexo	IV	Minuta do Contrato

DO OBJETO

1. A presente licitação tem como objeto a contratação de empresa especializada para o fornecimento de licenças *Kaspersky Endpoint Security for Business Select*, com Upgrade para a versão NEXT EDR OPTIMUM, de acordo com os termos e especificações deste edital e seus anexos.

2. A licitação será em lote único (grupo), conforme tabela constante do Termo de Referência.

3 . Em caso de discrepância entre as especificações deste objeto descritas no sistema compras.gov.br e as constantes deste edital, prevalecerão as do edital.

VALOR E DOTAÇÃO ORÇAMENTÁRIA

4 . O valor máximo aceitável para a contratação da totalidade do objeto desta licitação é de R$ 247.393,50 (duzentos e quarenta e sete mil trezentos e noventa e três reais e cinquenta centavos), conforme anexo dos Valores Máximos Admissíveis.

5 . As despesas pertinentes ao objeto do presente Edital correrão à conta da Fonte 1.5.00.100000, Subação 001369 (Manutenção, Serviços e Equipamento de Informática), Naturezas de Despesa 33.90.40.11 - Locação de Softwares e 33.90.40.08 - Manutenção de Softwares, do Orçamento da Alesc.

DAS CONDIÇÕES DE PARTICIPAÇÃO

6. Poderão participar da presente licitação os interessados que satisfaçam as condições estabelecidas neste Edital e em seus Anexos, e que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores (SICAF) e no Sistema eletrônico de compras (www.compras.gov.br).

7 . É de responsabilidade do cadastrado conferir a exatidão dos seus dados cadastrais nos Sistemas relacionados no item anterior e mantê-los atualizados junto aos órgãos responsáveis pela informação, devendo proceder, imediatamente, à correção ou à alteração dos registros tão logo identifique incorreção ou aqueles se tornem desatualizados.

8. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.

9. Os licitantes responsabilizam-se exclusiva e formalmente pelas transações efetuadas em seu nome, assumindo como firmes e verdadeiras suas propostas e lances, inclusive os atos praticados diretamente ou por seu representante, não cabendo ao provedor do sistema ou à Alesc a responsabilidade por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

10. O Licitante arcará integralmente com todos os custos de preparação e apresentação de sua proposta de preços, independentemente do resultado do procedimento licitatório.

11. Não poderá disputar esta licitação:

a) aquele que não atenda às condições deste Edital e de seus anexos;

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

c) 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 licitação versar sobre serviços ou fornecimento de bens a ela necessários;

d) Equiparam-se aos autores do projeto as empresas integrantes do mesmo grupo econômico.

e) pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

f) aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente da Alesc 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;

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

h) pessoa física ou jurídica que, nos 5 (cinco) anos anteriores à divulgação do edital, 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;

i) agente público vinculado à Alesc;

j) pessoas jurídicas reunidas em consórcio;

k) empresas concordatárias ou cuja falência tenha sido declarada, que se encontram sob concurso de credores, em dissolução ou em liquidação;

l) empresas que incorrerem em outros impedimentos previstos em Lei;

12. A participação neste Pregão importa para o Licitante a aceitação das condições estabelecidas no presente Edital, bem como a observância dos regulamentos, normas administrativas e técnicas aplicáveis, inclusive quanto aos recursos.

DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

13. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.

14. O Licitante deverá cadastrar proposta exclusivamente por meio do sistema eletrônico, até a data e o horário estabelecidos para abertura da sessão pública.

15. O Licitante deverá consignar, de forma expressa no sistema eletrônico, **o valor total ofertado pelo lote único (grupo)**, em reais (R$), com até duas casas decimais, já considerados e inclusos todos os tributos, descontos, fretes, tarifas e demais despesas decorrentes da execução do objeto.

16. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema,

que:

a) cumpre a cota de aprendizagem nos termos estabelecidos no art. 429 da CLT;

b) a proposta apresentada foi elaborada de forma independente e o conteúdo da proposta não foi, no todo ou em parte, direta ou indiretamente, informado, discutido ou recebido por qualquer outro participante potencial ou de fato, por qualquer meio ou por qualquer pessoa;

c) está ciente e concorda com as condições contidas no Edital e seus anexos, bem como de que cumpre plenamente os requisitos de habilitação definidos no edital;

d) não possui em sua cadeia produtiva, empregados executando trabalho degradante ou forçado, nos termos do inciso III e IV do art. 1° e no inciso III do art. 5º da Constituição Federal;

e) 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;

f) não ultrapassou o limite de faturamento e cumpre os requisitos estabelecidos do art. 3º da Lei Complementar n° 123, de 14 de dezembro de 2006, sendo apto a usufruir do tratamento favorecido estabelecido nos artigos 42 e 40 da referida Lei Complementar;

g) que, conforme disposto no art. 93 da Lei n° 8.213, de 24 de julho de 1991, está ciente do cumprimento da reserva de cargos prevista em lei para pessoas com deficiência ou para reabilitado da Previdência Social e que, se aplicado ao número de funcionários da empresa, atende as regras de acessibilidade previstas na legislação;

h) que até a presente data inexistem fatos impeditivos para sua habilitação no presente processo licitatório, ciente da obrigatoriedade de declarar ocorrências posteriores;

17. Ao cadastrar a proposta no sistema eletrônico, a Licitante declara, além do previsto no próprio sistema, que está em conformidade com as exigências estabelecidas pelas Leis Estaduais nº 10.732, de 07/04/1998, e nº 16.003, de 25/04/2013, sendo esta última regulamentada pelo Decreto Estadual nº 1.694, de 23/08/2013.

18. Ao cadastrar a proposta no sistema eletrônico a Licitante também se obriga a respeitar todas as condições previstas na Lei n° 13.709/2018 (Lei Geral de Proteção de Dados Pessoais).

19. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021.

20. No item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item.

21. Nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na Lei Complementar nº 123, de 2006, mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

22. A falsidade da declaração de que tratam os itens anteriores sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021 e neste Edital.

23. Os licitantes poderão retirar ou substituir a proposta até a abertura da sessão pública.

24. Qualquer elemento que possa identificar o licitante importará desclassificação da proposta,

sem prejuízo das sanções previstas neste edital.

ABERTURA DA SESSÃO PÚBLICA

25. A abertura da sessão pública deste Pregão, conduzida pelo Pregoeiro, ocorrerá na data e na hora indicadas no preâmbulo deste Edital, no Portal de Compras do Governo Federal, no sistema www.compras.gov.br.

26. Durante a sessão pública, a comunicação entre o Pregoeiro e os licitantes ocorrerá exclusivamente mediante troca de mensagens, em campo próprio do sistema eletrônico.

27. Cabe ao Licitante acompanhar as operações no sistema eletrônico durante a sessão pública do Pregão, ficando responsável pelo ônus decorrente da perda de negócios diante da inobservância de qualquer mensagem emitida pelo sistema ou de sua desconexão.

DA CLASSIFICAÇÃO DAS PROPOSTAS

28. As propostas cadastradas pelos licitantes no sistema eletrônico que descumprirem as exigências do edital quanto à forma de sua apresentação e/ou apresentarem erros que prejudiquem a oferta de lances e o caráter competitivo do certame também serão desclassificadas, mediante decisão fundamentada do Pregoeiro.

29. Somente os licitantes com propostas classificadas participarão da fase de lances.

DA FORMULAÇÃO DE LANCES

30. Aberta a etapa competitiva, os licitantes classificados poderão encaminhar lances sucessivos, exclusivamente por meio do sistema eletrônico, sendo imediatamente informados do horário e valor consignados no registro de cada lance.

31. O Licitante somente poderá oferecer lance inferior ao último por ele ofertado e registrado no sistema eletrônico, respeitado o intervalo mínimo de diferença de valores entre os lances que deverá ser de 0,1% (um décimo por cento) que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta.

32. Será adotado para o envio de lances no pregão eletrônico o modo de disputa **ABERTO**, em que os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

33. A etapa de lances da sessão pública terá duração de 10 (dez) minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos 2 (dois) minutos do período de duração da sessão pública.

34. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de 2 (dois) minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários.

35. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente.

36. No caso de desconexão com o Pregoeiro, no decorrer da etapa competitiva do Pregão, o sistema eletrônico poderá permanecer acessível aos licitantes para a recepção dos lances.

37. No caso de a desconexão do Pregoeiro persistir por tempo superior a 10 (dez) minutos, a sessão do pregão será suspensa automaticamente e terá reinício somente após comunicação expressa aos participantes no sítio www.compras.gov.br.

38. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.

39. Havendo eventual empate entre propostas ou lances, o critério de desempate será a reabertura para disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação.

40. Persistindo o empate mencionado no item anterior os critérios serão aqueles estabelecidos na legislação vigente.

DO BENEFÍCIO ÀS MICROEMPRESAS E ÀS EMPRESAS DE PEQUENO PORTE

41. A obtenção de benefícios previstos dos artigos 42 a 49 da Lei Complementar n. 123/2006 fica limitada às microempresas e às empresas de pequeno porte que, no ano-calendário de realização da licitação, ainda não tenham celebrado contratos com a Administração Pública cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte, devendo o licitante apresentar declaração de observância desse limite.

42. Após a fase de lances, se a proposta mais bem classificada não tiver sido apresentada por microempresa ou empresa de pequeno porte apta a usufruir dos benefícios e se houver proposta de microempresa ou empresa de pequeno porte igual ou até 5% (cinco por cento) superior à proposta mais bem classificada, se procederá da seguinte forma:

a) a microempresa ou a empresa de pequeno porte mais bem classificada poderá, no prazo de 5 (cinco) minutos, apresentar proposta de preço inferior à do licitante mais bem classificado e, se atendidas as exigências deste edital, ser adjudicatária;

b) não sendo adjudicatária a microempresa ou empresa de pequeno porte mais bem classificada na forma do subitem anterior, e havendo outros licitantes que se enquadrem na condição prevista no caput deste item, estes serão convocados, na ordem classificatória, para o exercício do mesmo direito;

c) o convocado que não apresentar proposta dentro do prazo de 5 (cinco) minutos, controlado pelo sistema eletrônico, decairá do direito previsto nos artigos 44 e 45 da Lei Complementar n. 123/2006.

43. Na hipótese de não adjudicação nos termos previstos nesta cláusula, o procedimento licitatório prosseguirá com os demais licitantes.[LU5]

DA NEGOCIAÇÃO

44. O Pregoeiro deverá encaminhar contraproposta diretamente ao licitante que tenha apresentado o lance mais vantajoso, observados o critério de julgamento e o valor estimado para a contratação.

45. A negociação será realizada por meio do sistema eletrônico e poderá ser acompanhada pelos demais licitantes.

DA ACEITABILIDADE DA PROPOSTA

46. O julgamento da proposta de preços dar-se-á pelo critério de **MENOR PREÇO POR LOTE ÚNICO (GRUPO)**, observadas as especificações técnicas e os parâmetros definidos no Edital.

47. A proposta de preços original devidamente atualizada com o último lance ofertado após a negociação e assinada pelo representante da empresa, conforme anexo da Proposta Comercial, bem como outros documentos complementares eventualmente necessários, deverão ser encaminhados via sistema, em até 2 (duas) horas, contadas da solicitação do Pregoeiro.

48. O Pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor máximo estipulado para o lote único (grupo), bem como dos itens que individualmente o compõem e à compatibilidade da proposta com as especificações técnicas do objeto, conforme disposições contidas no presente Edital.

49. Se a proposta não for aceitável, ou se o licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este Edital, sendo o respectivo licitante declarado vencedor pelo Pregoeiro.

50. O Pregoeiro poderá solicitar parecer de técnicos pertencentes ao quadro de pessoal da Alesc ou, ainda, de pessoas físicas ou jurídicas (às suas expensas) externas, para orientar sua decisão.

51. Não se considerará qualquer oferta de vantagem não prevista neste edital.

52. Não se admitirá proposta que apresente valores simbólicos, irrisórios ou de valor zero, incompatíveis com os preços de mercado, exceto quando se referirem a materiais e instalações de propriedade do licitante, para os quais ela renuncie à parcela ou à totalidade de remuneração.

53. Não se admitirá preço global superior ao orçamento estimado ou com preços manifestamente inexequíveis.

54. As propostas não poderão apresentar preços unitários superiores aos constantes na planilha orçamentária da Alesc ou com preços manifestamente inexequíveis.

55. Os critérios de aceitabilidade são cumulativos, verificando-se tanto o valor global quanto os valores unitários estimativos da contratação.

56. Considerar-se-á inexequível a proposta que não venha a ter demonstrada sua viabilidade por meio de documentação que comprove que os custos envolvidos na contratação são coerentes com os de mercado do objeto deste pregão.

57. Será desclassificada a proposta que não corrigir ou não justificar eventuais falhas apontadas pelo Pregoeiro, sujeitando-se às sanções previstas neste instrumento convocatório.

58. Não serão motivo de desclassificação simples omissões que sejam irrelevantes para o entendimento da Proposta de Preços, que não venham causar prejuízo para a Alesc ou firam os direitos dos demais licitantes.

59. A indicação do lance vencedor, a classificação dos lances apresentados e demais informações relativas à sessão pública do Pregão Eletrônico constarão de ata divulgada no sistema eletrônico, sem prejuízo das demais formas de publicidade previstas na legislação pertinente.

DA HABILITAÇÃO

60. Os documentos de habilitação deverão ser encaminhados no prazo estipulado pelo Pregoeiro, exclusivamente por meio do sistema eletrônico.

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

a) SICAF;
b) Cadastro Nacional de Empresas Inidôneas e Suspensas (CEIS);
c) Cadastro Nacional de Empresas Punidas (CNEP);
d) Cadastro Nacional de Condenações Cíveis por Atos de Improbidade Administrativa;
e) Lista de Inidôneos, mantida pelo Tribunal de Contas da União;
f) Cadastro de Fornecedores da Secretaria de Estado da Administração do Estado de Santa Catarina (http://www.portaldecompras.sc.gov.br).

62. A consulta aos cadastros acima mencionados será realizada em nome da empresa licitante e de seu sócio majoritário, por força do art. 12 da Lei nº 8.429/1992.

63. A habilitação dos licitantes será verificada por meio do SICAF, bem como da documentação complementar especificada neste edital.

64. Os licitantes deverão encaminhar, no prazo estipulado pelo Pregoeiro, via sistema eletrônico, a seguinte documentação complementar relativa à **habilitação econômico-financeira**:

a) certidão negativa da falência expedida pelo distribuidor da sede do licitante ;

65. Os licitantes deverão encaminhar, no prazo estipulado pelo Pregoeiro, via sistema eletrônico, a seguinte documentação complementar relativa à **habilitação técnica**:

a) Comprovação de aptidão para a prestação dos serviços compatíveis com o objeto desta contratação, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado:

i) O licitante deverá fornecer atestados que comprovem o fornecimento de ao menos 300 (trezentas) licenças.

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

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

b) Certificado que comprove que a Licitante é revendedora oficial da marca oferecida, comprovando através de carta do fabricante.

66. Quando não constante no SICAF, o licitante deverá apresentar a seguinte documentação relativa à **habilitação jurídica**, conforme o caso:

a) cédula de identidade, no caso de licitante pessoa física;

b) registro comercial, no caso de empresa individual;

c) ato constitutivo, estatuto ou contrato social em vigor, devidamente registrado, em se tratando de sociedades comerciais, e, no caso de sociedades por ações, acompanhado de documentos de eleição de seus administradores;

d) inscrição do ato constitutivo, no caso de sociedades civis, acompanhada de prova de diretoria em exercício;

e) decreto de autorização, em se tratando de empresa ou sociedade estrangeira em funcionamento no País, e ato de registro ou autorização para funcionamento expedido pelo órgão competente, quando a atividade assim o exigir.

67. Quando não constante no SICAF, o licitante deverá apresentar a seguinte documentação relativa à **habilitação fiscal e trabalhista**:

a) prova de inscrição no Cadastro de Pessoas Físicas (CPF) ou no Cadastro Nacional da Pessoa Jurídica (CNPJ);

b) prova de regularidade perante a Fazenda Federal;

c) prova de regularidade perante a Fazenda Estadual;

d) caso o Licitante seja de outro Estado da Federação, deverá apresentar, também, a prova de regularidade para com a Fazenda do Estado de Santa Catarina, nos termos dos Decretos estaduais nºs 3.650/93 e 3.884/93;

e) prova de regularidade perante a Fazenda Municipal do domicílio ou sede do licitante;

f) prova de regularidade com o FGTS;

g) prova de regularidade com a Justiça do Trabalho;

h) certidão negativa de efeitos de falência, recuperação judicial ou recuperação extrajudicial expedida pelo distribuidor da sede do licitante.

68. Os licitantes que não atenderem às exigências de habilitação com as informações constantes no SICAF deverão encaminhar, via sistema eletrônico, no prazo fixado pelo Pregoeiro, documentos que supram tais exigências, na forma do art. 70 da Lei n. 14.133/2021.

69. O Pregoeiro poderá consultar sítios oficiais de órgãos e entidades emissores de certidões para verificar as condições de habilitação dos licitantes.

70. As declarações exigidas neste edital poderão ser supridas mediante manifestação expressa do licitante no chat do sistema compras.gov.br.

71. Havendo a necessidade de envio de documentos para a confirmação daqueles exigidos neste edital e já apresentados, ou, ainda, de envio de documentos não juntados, mas que comprovem que na data da apresentação da proposta o licitante atendia às condições de aceitabilidade da proposta e de habilitação, o licitante será convocado a encaminhá-los, via sistema eletrônico, no prazo fixado pelo Pregoeiro, sob pena de desclassificação ou de

inabilitação, prazo durante o qual a sessão não será suspensa.

72. Sob pena de inabilitação, os documentos encaminhados deverão estar em nome do licitante, com indicação precisa de dados capazes de qualificar inequivocamente o licitante.

73. Em se tratando de filial, os documentos de habilitação jurídica e regularidade fiscal deverão estar em nome da filial, exceto aqueles que, pela própria natureza, são emitidos somente em nome da matriz.

74. Em se tratando de microempresa ou empresa de pequeno porte, havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 05 (cinco) dias úteis, cujo termo inicial corresponderá ao momento em que o proponente for declarado vencedor do certame, prorrogável por igual período, a critério da Administração, para a regularização da documentação, pagamento ou parcelamento do débito, e emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

75. A não regularização da documentação no prazo previsto no subitem anterior implicará decadência do direito à contratação, sem prejuízo das sanções previstas neste edital, e facultará ao Pregoeiro convocar os licitantes remanescentes, na ordem de classificação.

76. Se a proposta for desclassificada ou, ainda, se o licitante não atender às exigências de habilitação, o Pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a seleção da proposta que melhor atenda a este edital.

77. Constatado o atendimento às exigências fixadas neste edital, o licitante será declarado o vencedor.

78. Para o documento no qual não conste prazo de validade será considerado o prazo de 90 (noventa) dias, a contar da data da sua emissão, salvo para aqueles que, por sua própria natureza, não apresentem prazo de validade, como é o caso dos atestados de capacidade técnica.

DO RECURSO

79. Caberá recurso em face de julgamento das propostas, ato de habilitação ou inabilitação de licitante, anulação ou revogação da licitação.

80. Após a fase de julgamento o sistema abrirá prazo de 10 (dez) minutos, durante o qual, qualquer licitante poderá, em campo próprio do sistema, manifestar sua intenção de recurso.

81. Em seguida, após a fase de habilitação, o sistema abrirá prazo de 10 (dez) minutos, durante o qual, qualquer licitante poderá, em campo próprio do sistema, manifestar sua intenção de recurso.

82. O prazo para apresentação das razões recursais será de 3 (três) dias úteis e será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação.

83. A apreciação se dará em fase única.

84. A falta de manifestação no prazo estabelecido autoriza a Administração a adjudicar o objeto ao licitante vencedor.

DA ADJUDICAÇÃO E HOMOLOGAÇÃO

85. O objeto deste pregão será adjudicado ao licitante vencedor.

86. A homologação deste Pregão compete ao Diretor Geral da Alesc ou ao Diretor de Comunicação Social, conforme o caso e em atenção aos termos contidos no Ato da Mesa nº 195, de 16 de junho de 2020.

DO INSTRUMENTO CONTRATUAL

87. Depois de homologado o resultado deste Pregão, o licitante vencedor será convocado para se cadastrar no sistema SEI e, em seguida, assinar o contrato, e terá o prazo de até 5 (cinco) dias úteis para concluir o cadastro e efetuar a assinatura, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital e na Lei n° 14.133/2021.

88. O prazo para assinatura do contrato poderá ser prorrogado uma única vez, por igual período, quando solicitado pelo licitante vencedor durante o seu transcurso, desde que ocorra motivo justificado e aceito pela Alesc.

89. O licitante deverá manter atualizado o seu endereço de *e-mail* junto à Alesc e confirmar o recebimento das mensagens provenientes dela, não podendo alegar o desconhecimento do recebimento das comunicações por este meio como justificativa para se eximir das responsabilidades assumidas ou eventuais sanções aplicadas.

90. Os representantes legais deverão realizar seu cadastro para obter seu login e senha para assinatura eletrônica do contrato ou ata de registro de preços, por meio do sistema SEI, no seguinte endereço eletrônico: https://sei.alesc.sc.gov.br/sei/controlador_externo.php?acao=usuario_externo_logar&id_orgao_acesso_externo=0 .

91. O pedido de credenciamento de usuário externo ao SEI é ato pessoal e intransferível e, portanto, não serão aceitos cadastros de e-mails setoriais, somente e-mails pessoais.

92. Dúvidas referentes ao cadastro no sistema SEI deverão ser solucionadas no e-mail sei@alesc.sc.gov.br e/ou pelo telefone (48) 3221-2532.

93. Os encargos das partes e as normas relativas a recebimento, liquidação, pagamento, alteração e rescisão contratual constam do Termo de Referência e/ou minuta do contrato encartado neste Edital.

94. Por ocasião da assinatura do contrato, será verificado no SICAF e em outros meios se o adjudicatário mantém as condições de habilitação.

DAS SANÇÕES ADMINISTRATIVAS

95. As sanções administrativas às quais o licitante estará sujeito estão previstas no Termo de Referência e na minuta do contrato, encartados neste Edital.

DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

96. Até 03 (três) dias úteis antes da data fixada para abertura da sessão pública, qualquer pessoa, física ou jurídica, poderá impugnar o ato convocatório deste Pregão, mediante petição a ser enviada exclusivamente para o endereço eletrônico licitacoes@alesc.sc.gov.br.

97. O Pregoeiro, auxiliado pelo setor técnico, pela Coordenadoria de Licitações e Contratos, ou pela Equipe de Planejamento, decidirá sobre a impugnação do certame.

98. Acolhida a impugnação contra este Edital, será designada e publicada nova data para a realização do certame, exceto quando, inquestionavelmente, a alteração não afetar a formulação das propostas.

99. Os pedidos de esclarecimentos devem ser enviados ao Pregoeiro até 03 (três) dias úteis antes da data fixada para abertura da sessão pública, exclusivamente para o endereço eletrônico licitacoes@alesc.sc.gov.br.

100. As respostas às impugnações e aos esclarecimentos solicitados serão disponibilizadas no sistema eletrônico em até 3 (três) dias úteis, contados do recebimento do pedido, limitado ao último dia útil anterior à data da abertura do certame.

DISPOSIÇÕES FINAIS

101. É facultado ao Pregoeiro ou à autoridade superior, em qualquer fase deste Pregão promover diligência destinada a esclarecer ou completar a instrução do processo, vedada a inclusão posterior de informação ou de documentos que deveriam ter sido apresentados para fins de classificação e habilitação, salvo se tratar-se de informação complementar, conforme disposto no artigo 64 da Lei n° 14.133/2021.

102. No julgamento das propostas e na fase de habilitação, o Pregoeiro poderá sanar erros ou falhas que não alterem a substância das propostas e dos documentos e sua validade jurídica, mediante despacho fundamentado, registrado em ata e acessível a todos, atribuindo-lhe validade e eficácia para fins de classificação e habilitação.

103. Caso os prazos definidos neste Edital não estejam expressamente indicados na proposta, eles serão considerados como aceitos para efeito de julgamento deste Pregão.

104. Poderá ser solicitada tradução para a língua portuguesa, efetuada por tradutor juramentado, de documentos emitidos em língua estrangeira, que também deverão ser devidamente consularizados ou registrados em cartório de títulos e documentos.

105. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerão as deste Edital.

106. Este pregão poderá ter a data de abertura da sessão pública transferida por conveniência da Alesc.

107. Na contagem dos prazos estabelecidos neste edital, será excluído o dia do início e incluído o do vencimento, e serão considerados os dias consecutivos, exceto quando for explicitamente disposto em contrário.

108. Só se iniciam e vencem os prazos referidos nesta licitação em dia de expediente na Alesc,

portanto serão prorrogados até o próximo dia útil os prazos que vencerem durante dias sem expediente.

109. Qualquer comunicação pertinente a este processo licitatório a ser realizada entre a Alesc e terceiros deve ocorrer por escrito, preferencialmente por e-mail, sendo que os prazos indicados nas comunicações se iniciam em 2 (dois) dias úteis a contar da data de envio do e-mail, salvo se houver confirmação de leitura ou de recebimento anterior, hipótese em que os prazos se iniciam com a respectiva confirmação.

110. Integra o presente edital a minuta do contrato.

111. Em caso de dúvidas relacionadas ao sistema Compras.gov.br, o licitante deverá entrar em contato com o suporte do sistema, através do telefone **0800-978-9001**, ou do site **portaldeservicos.economia.gov.br** (suporte realizado de segunda a sexta-feira, das 07h às 20h).

DO FORO

112. As questões decorrentes da execução deste instrumento que não possam ser dirimidas administrativamente serão processadas e julgadas no Foro da Comarca da Capital, no Município de Florianópolis, do Estado de Santa Catarina, com a renúncia expressa de qualquer outro.

Florianópolis, data da assinatura eletrônica do edital.

_____

Leonardo Lorenzetti
Diretor-Geral

_____

Carlos Alberto Leal
Coordenador de Licitações e Contratos

ANEXO I

EDITAL DE PREGÃO ELETRÔNICO Nº 005/2025

TERMO DE REFERÊNCIA

1. INFORMAÇÕES BÁSICAS

Processo: SEI n° 24.0.000044917-9

Área Requisitante: Gerência de Segurança e Administração de Redes

Fundamento Legal: Ato de Mesa n° 257/2024 e Lei n°14.133/2021

2. OBJETO

2.1. Contratação de empresa especializada para o fornecimento de licenças *Kaspersky Endpoint Security for Business Select*, com Upgrade para a versão NEXT EDR OPTIMUM, de acordo com os termos e especificações deste edital e seus anexos.

Item	Especificação	Unidade	CATSER	Quantidade Total
01	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT com Upgrade para a versão NEXT EDR OPTIMUM	Unid	350949	1.150
02	Serviço de suporte técnico incluindo instalação, configuração, treinamento básico e atendimento “online” e “on site”	mês	350949	36

2.2. Solução de segurança cibernética que utiliza tecnologias avançadas de detecção, aprendizado de máquina e análise comportamental para identificar e neutralizar ameaças em tempo real contra malware, phishing, ransomware e ataques de rede. ferramentas incluem firewall integrado, VPN, controle de vulnerabilidades e módulos de proteção para endpoints e servidores.

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

2.4. Os bens objeto desta contratação são caracterizados como comuns, com características e especificações usuais de mercado.

3. VIGÊNCIA

3.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses, contados da assinatura do contrato, prorrogável por até 10 anos, na forma do artigo 107 da Lei n° 14.133/2021.

3.2. O serviço é enquadrado como continuado tendo em vista que a proteção contra ameaças cibernéticas, como vírus, malwares e outras vulnerabilidades, é uma necessidade constante e ininterrupta para garantir a segurança dos sistemas e dados institucionais. O antivírus desempenha um papel essencial na manutenção da integridade, confidencialidade e disponibilidade das informações, exigindo atualizações regulares e suporte técnico contínuo para acompanhar a evolução das ameaças digitais.

3.3. Além disso, a utilização de um serviço de antivírus envolve licenças periódicas e suporte especializado, que garantem a eficácia das soluções implantadas e a resolução ágil de incidentes

de segurança, caracterizando sua natureza como serviço indispensável e permanente no âmbito da proteção tecnológica.

4. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

4.1. Conforme fundamentado na análise comparativa das soluções no Estudo Técnico Preliminar, a alternativa viável consiste na aquisição de solução de segurança de proteção Kaspersky Endpoint Security for Business Select com upgrade para a versão Next Edr Optimum.

Esse serviço compreende atividades de suporte e atualizações da solução existente, de forma a manter as condições operacionais da rede de dados corporativa.

5. CARACTERÍSTICAS TÉCNICAS

5.1. Do módulo de proteção de endpoint:

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

5.1.1.1. Windows 7;

5.1.1.2. Windows 8;

5.1.1.3. Windows 8.1;

5.1.1.4. Windows 10;

5.1.1.5. Windows 11 e posterior.

5.1.2. Servidores:

5.1.2.1. Windows Small Business Server 2011;

5.1.2.2. Windows MultiPoint Server 2011;

5.1.2.3. Windows Server 2008 R2, 2012 R2, 2016, 2019 e 2022;

5.1.2.4. Servidores de terminal Microsoft;

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

5.1.3. Sistemas operacionais Linux de 32 bits:

5.1.3.1. CentOS 6.7 e posterior;

5.1.3.2. Debian GNU/Linux 11.0 e posterior;

5.1.3.3. Debian GNU/Linux 12.0 e posterior;

5.1.3.4. Red Hat Enterprise Linux 6.7 e posterior;

5.1.4. Sistemas operacionais Linux de 64 bits.

5.1.4.1. Amazon Linux 2;

5.1.4.2. CentOS 6.7 e mais tarde;

5.1.4.3. CentOS 7.2 e posterior;

5.1.4.4. CentOS Stream 8;

5.1.4.5. CentOS Stream 9;

5.1.4.6. Debian GNU/Linux 11.0 e posterior;

5.1.4.7. Debian GNU/Linux 12.0 e posterior;

5.1.4.8. Linux Mint 20.3 e superior;

5.1.4.9. Linux Mint 21.1 e posterior;

5.1.4.10. openSUSE Leap 15.0 e posterior;

5.1.4.11. Oracle Linux 7.3 e posterior;

5.1.4.12. Oracle Linux 8.0 e posterior;

5.1.4.13. Oracle Linux 9.0 e posterior;

5.1.4.14. Red Hat Enterprise Linux 6.7 e posterior;

5.1.4.15. Red Hat Enterprise Linux 7.2 e posterior;

5.1.4.16. Red Hat Enterprise Linux 8.0 e posterior;

5.1.4.17. Red Hat Enterprise Linux 9.0 e posterior;

5.1.4.18. Rocky Linux 8.5 e posterior;

5.1.4.19. Rocky Linux 9.1;

5.1.4.20. SUSE Linux Enterprise Server 12.5 ou posterior;

5.1.4.21. SUSE Linux Enterprise Server 15 ou posterior;

5.1.4.22. Ubuntu 20.04 LTS;

5.1.4.23. Ubuntu 22.04 LTS;

5.1.4.24. Sistemas operacionais Arm de 64 bits;

5.1.4.25. CentOS Stream 9;

5.1.4.26. SUSE Linux Enterprise Server 15;

5.1.4.27. Ubuntu 22.04 LTS;

5.1.5. Sistemas operacionais MAC OS:

5.1.5.1. macOS 12 – 14 e posterior;

5.1.6. Ferramentas de virtualização MAC OS:

5.1.6.1. Parallels Desktop 16 para Mac Business Edition;

5.1.6.2. VMware Fusion 11.5 Profissional;

5.1.6.3. VMware Fusion 12 Profissional.

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

5.1.7.1. VMware Workstation 17.0.2 Pro;

5.1.7.2. VMware ESXi 8.0 Update 2;

5.1.7.3. Microsoft Hyper-V Server 2019;

5.1.7.4. Citrix Virtual Apps e Desktop 7 2308;

5.1.7.5. Citrix Provisioning 2308;

5.1.7.6. Citrix Hypervisor 8.2 Update 1.

5.2. **Do módulo de gerenciamento avançado**

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

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

5.2.2.1. Amazon Web Services;

5.2.2.2. Microsoft Azure;

5.2.2.3. Google Cloud.

5.2.3. A solução proposta deve incluir as seguintes opções de integração SIEM:

5.2.3.1. HP (Microfoco) ArcSight;

5.2.3.2. IBM QRadar;

5.2.3.3. Splunk;

5.2.3.4. Kaspersky KUMA.

5.3. 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.

5.4. 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.

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

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

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

5.8. 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.

5.9. 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.

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

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

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

5.13. 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:

5.13.1. Status do dispositivo;

5.13.2. Tag;

5.13.3. Diretório ativo;

5.13.4. Proprietários de dispositivos;

5.13.5. Hardware.

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

5.14.1. E-mail;

5.14.2. Registro de sistema;

5.14.3. SMS.

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

5.15.1. Atributos de rede;

5.15.2. Nome;

5.15.3. Domínio e/ou Sufixo de Domínio;

5.15.4. Endereço de IP;

5.15.5. Endereço IP para servidor de gerenciamento;

5.15.6. Localização no Active Directory;

5.15.7. Unidade organizacional;

5.15.8. Grupo;

5.15.9. Sistema operacional;

5.15.10. Número do pacote de serviço;

5.15.11. Arquitetura Virtual;

5.15.12. Registro de aplicativos;

5.15.13. Nome da Aplicação;

5.15.14. Versão do aplicativo;

5.15.15. Fabricante;

5.15.16. Tipo e versão;

5.15.17. Arquitetura.

5.16. 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.

5.17. 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.

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

5.18.1. Dispositivos Desktop/Servidores;

5.18.2. Dispositivos móveis;

5.18.3. Dispositivos de rede;

5.18.4. Dispositivos virtuais;

5.18.5. Componentes OEM;

5.18.6. Periféricos de computador;

5.18.7. Dispositivos IoT conectados;

5.18.8. Telefones VoIP;

5.18.9. Repositórios de rede.

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

5.19.1. Nome da Aplicação;

5.19.2. Caminho do aplicativo;

5.19.3. Metadados do aplicativo;

5.19.4. Aplicativo Certificado digital;

5.19.5. Categorias de aplicativos predefinidas pelo fornecedor SHA256 e MD5.

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

5.20.1. Bluetooth;

5.20.2. Dispositivos móveis;

5.20.3. Modems externos;

5.20.4. CD/DVD;

5.20.5. Câmeras e scanners;

5.20.6. MTPs;

5.20.7. E a transferência de dados para dispositivos móveis.

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

5.22. A solução proposta 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.

5.23. 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:

5.23.1. Estruturas de domínios e grupos de trabalho do Windows;

5.23.2. Estruturas de grupos do Active Directory;

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

5.24. 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.

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

5.25.1. Verificação manual;

5.25.2. Verificação no acesso;

5.25.3. Verificação por demanda;

5.25.4. Verificação de arquivos compactados;

5.25.5. Verificação de arquivos individuais, pastas e unidades;

5.25.6. Bloqueio e verificação de scripts;

5.25.7. Proteção contra alteração de registros;

5.25.8. Proteção contra estouro de buffer;

5.25.9. Verificação em segundo plano/inativa;

5.25.10. Verificação de unidade removível na conexão com o sistema.

5.26. 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.

5.27. 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.

5.28. 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.

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

5.30. 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.

5.31. A solução proposta deve suportar Windows Failover Cluster.

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

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

5.34. 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.

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

5.36. 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.

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

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

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

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

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

5.42. 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.

5.43. 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.

5.44. 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).

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

5.46. 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.

5.47. 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.

5.48. 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.

5.49. 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.

5.50. A solução proposta deve dar acesso aos serviços em nuvem do fornecedor de segurança anti-malware através do servidor de administração.

5.51. A solução proposta deve ser capaz de realizar inventários de software e hardware instalados nos computadores dos usuários.

5.52. A solução proposta deve ter um mecanismo de notificação para informar os usuários sobre eventos no software e nas configurações anti-malware instalados, e para distribuir notificações sobre eventos por e-mail.

5.53. A solução proposta deve permitir a instalação centralizada de aplicativos de terceiros em todos ou em computadores selecionados.

5.54. 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.

5.55. 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. .

5.56. 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.

5.57. 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 definido. Os valores para o número de vírus e escala de tempo devem ser configuráveis.

5.58. A solução proposta deve permitir ao administrador personalizar relatórios.

5.59. 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.

5.60. 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.

5.61. A solução proposta deve permitir ao administrador definir diferentes condições de mudança de status para grupos de endpoint no servidor de gerenciamento.

5.62. A solução proposta deve permitir que o administrador adicione ferramentas de gerenciamento de endpoint personalizadas/de terceiros ao servidor de gerenciamento.

5.63. 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.

5.64. A funcionalidade 'Dispositivo desativado' deve estar disponível, para que tais dispositivos não sejam exibidos na lista de equipamentos.

5.65. 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;

5.66. 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.

5.67. A solução proposta deve suportar integração com solução APT(Advanced Persistent Threat).

5.68. A solução proposta deve suportar a integração com o serviço Managed Detection and Response.

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

5.69.1. Windows;

5.69.2. Linux.

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

5.70.1. Windows;

5.70.2. Microsoft SQL Server;

5.70.3. Microsoft Banco de dados SQL do Azure;

5.70.4. MySQL Standard e Enterprise;

5.70.5. MariaDB;

5.70.6. PostgreSQL;

5.70.7. MySQL;

5.70.8. MariaDB;

5.70.8.1. PostgreSQL.

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

5.71.1. Windows:

5.71.1.1. VMware vSphere 6.7 e 7.0;

5.71.1.2. Estação de trabalho VMware 16 Pro;

5.71.1.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

5.71.1.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

5.71.1.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

5.71.1.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

5.71.1.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

5.71.1.8. Citrix XenServer 7.1 LTSR;

5.71.1.9. Citrix XenServer 8.x;

5.71.1.10. Oracle VM VirtualBox 6.x.

5.71.2. Linux:

5.71.2.1. VMware vSphere 6.7, 7.0 e 8.0;

5.71.2.2. VMware Desktop 16 Pro e 17 Pro;

5.71.2.3. Servidor Microsoft Hyper-V 2012 de 64 bits;

5.71.2.4. Servidor Microsoft Hyper-V 2012 R2 de 64 bits;

5.71.2.5. Microsoft Servidor Hyper -V 2016 de 64 bits;

5.71.2.6. Servidor Microsoft Hyper-V 2019 de 64 bits;

5.71.2.7. Servidor Microsoft Hyper-V 2022 de 64 bits;

5.71.2.8. Citrix XenServer 7.1 e 8.x;

5.71.2.9. Oracle VM VirtualBox 6.x e7.x.

5.72. A solução proposta deve suportar criptografia em vários níveis:

5.72.1. Criptografia completa do disco – incluindo disco do sistema;

5.72.2. Criptografia de arquivos e pastas;

5.72.3. Criptografia de mídia removível;

5.72.4. Gerenciamento de criptografia BitLocker e MacOS Filevault2.

5.73. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita:

5.73.1. A criptografia de arquivos em unidades de computador locais;

5.73.2. A criação de listas de criptografia de arquivos por extensão ou grupo de extensões;

5.73.3. A criação de listas criptografadas de pastas em unidades de computador locais.

5.74. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de arquivos em unidades removíveis. Isto deve incluir a capacidade de:

5.74.1. Especifique uma regra de criptografia padrão pela qual o aplicativo aplique a mesma ação a todas as unidades removíveis;

5.74.2. Configure regras de criptografia para arquivos armazenados em unidades removíveis individuais;

5.75. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que suporte vários modos de criptografia de arquivos para unidades removíveis:

5.75.1. A criptografia de todos os arquivos armazenados em unidades removíveis;

5.75.2. A criptografia de novos arquivos somente quando eles são salvos ou criados em unidades removíveis.

5.76. A solução proposta deve oferecer a funcionalidade Integrated File Level Encryption (FLE) que permite que os arquivos em unidades removíveis sejam criptografados em modo portátil. Deve permitir o acesso a arquivos criptografados em unidades removíveis conectadas a computadores sem funcionalidade de criptografia.

5.77. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita a criptografia de todos os arquivos que aplicativos específicos possam criar ou modificar, tanto em discos rígidos quanto em unidades removíveis.

5.78. A solução proposta deve oferecer funcionalidade integrada de criptografia em nível de arquivo (FLE) que permita o gerenciamento de regras de acesso de aplicativos a arquivos criptografados, incluindo a definição de uma regra de acesso a arquivos criptografados para qualquer aplicativo. Deve permitir o bloqueio do acesso a arquivos criptografados ou permitir o acesso a arquivos criptografados apenas como texto cifrado.

5.79. A solução proposta deve oferecer a capacidade de restaurar dispositivos criptografados se um disco rígido ou unidade removível criptografado estiver corrompido.

5.80. A solução proposta deve oferecer a funcionalidade Integrated Full Disk Encryption (FDE) para discos rígidos e unidades removíveis. Tal como acontece com o FLE, deve haver a capacidade de especificar uma regra de criptografia padrão pela qual o aplicativo aplica a mesma ação a todas as unidades removíveis ou de configurar regras de criptografia para unidades removíveis individuais.

5.81. A solução proposta deve oferecer um módulo de criptografia gerenciado centralmente em todos os computadores, com capacidade de impor políticas de criptografia e modificar/interromper configurações de criptografia.

5.82. A solução proposta deve oferecer a capacidade de monitorar centralmente o status da criptografia e gerar relatórios sobre computadores/dispositivos criptografados.

5.83. A solução proposta deve oferecer criptografia totalmente transparente para os usuários finais e que não tenha impacto adverso no desempenho e na utilização do sistema.

5.84. A solução proposta deve oferecer criptografia completa de disco que suporte o gerenciamento centralizado de usuários autorizados, incluindo adição, remoção e redefinição de senha. Somente usuários autorizados devem ter permissão para inicializar o disco criptografado.

5.85. A solução proposta deve ter a capacidade de bloquear o acesso de aplicativos a dados criptografados, se necessário.

5.86. A solução proposta deverá suportar a encriptação automática de dispositivos de armazenamento amovíveis e deverá ser capaz de impedir a cópia de dados para suportes não encriptados.

5.87. A solução proposta deve proporcionar a possibilidade de criação de contentores protegidos por palavra-passe que possam ser utilizados para o intercâmbio de dados com utilizadores externos.

5.88. A solução proposta deve fornecer um local central para armazenamento de chaves de criptografia e múltiplas opções de recuperação.

5.89. O servidor administrador/gerenciador da solução proposta deve ter a capacidade de descriptografar todos os dados criptografados. independentemente da localização e/ou usuário.

5.90. A solução proposta deve suportar layouts de teclado QWERTY e AZERTY para autorização de pré-inicialização.

5.91. A solução proposta deve fornecer a funcionalidade para gerenciar/aplicar a criptografia do Microsoft Bit Locker.

5.92. A solução proposta deve fornecer a funcionalidade para personalizar as configurações de criptografia do Microsoft BitLocker, incluindo:

5.92.1. Uso do Trusted Platform Module e configurações de senha;

5.92.2. Uso de criptografia de hardware para estações de trabalho e criptografia de software se a criptografia de hardware não estiver disponível.

5.93. Uso de autenticação que exige entrada de dados em um ambiente de pré-inicialização, mesmo que a plataforma não tenha capacidade para entrada de pré-inicialização (por exemplo, com teclados touchscreen em tablets).

5.94. A solução proposta deve suportar criptografia em Microsoft Surface Tablets.

5.95. A solução proposta deverá incluir recursos para gerenciar computadores remotamente, incluindo:

5.95.1. Instalação remota de software de terceiros;

5.95.2. Relatórios sobre software e hardware existentes;

5.95.3. Monitoramento para instalação de software não autorizado;

5.95.4. Remoção de software não autorizado.

5.96. A solução proposta deverá incluir recursos de gerenciamento de patches para sistemas operacionais Windows e para aplicativos de terceiros instalados.

5.97. A funcionalidade de gerenciamento de patches da solução proposta deve ser totalmente automatizada, com capacidade de detectar, baixar e enviar patches ausentes para endpoints.

5.98. A solução proposta deve fornecer a possibilidade de selecionar quais patches serão baixados/enviados para os endpoints, com base em sua criticidade.

5.99. A solução proposta deve ser capaz de detectar vulnerabilidades existentes em sistemas operacionais e outros aplicativos instalados e, em seguida, responder baixando/enviando automaticamente os patches necessários para os terminais.

5.100. A solução proposta deve fornecer relatórios abrangentes sobre vulnerabilidades descobertas e patches ausentes, bem como sobre endpoints e status de implantação de patches.

5.101. A solução proposta deve ter a capacidade de aplicar patches específicos com base na criticidade ou gravidade.

5.102. O servidor de gerenciamento da solução proposta deve ser configurável como uma fonte de atualizações para Microsoft Updates e aplicativos de terceiros.

5.103. A solução proposta deve incluir o aconselhamento sobre vulnerabilidade do fornecedor de

aplicativos, bem como do fornecedor de segurança.

5.104. A solução proposta deve permitir ao administrador aprovar atualizações.

5.105. A solução proposta deve ser capaz de identificar automaticamente patches ausentes em endpoints individuais e enviar apenas os que são necessários/ausentes.

5.106. A solução proposta deve suportar a agregação de patches para minimizar o número de atualizações necessárias.

5.107. A solução proposta deve notificar o administrador sobre quaisquer patches ausentes nos terminais assim que as informações relevantes estiverem disponíveis.

5.108. A solução proposta deverá proporcionar a possibilidade de gerir separadamente a aplicação de patches para sistemas operativos e para aplicações de terceiros.

5.109. A solução proposta deverá proporcionar a possibilidade de corrigir vulnerabilidades existentes em qualquer ponto final ou apenas em pontos específicos.

5.110. A solução proposta deve fornecer a facilidade de detectar/instalar automaticamente todos os patches perdidos anteriormente que são necessários para aplicar o patch selecionado (dependências).

5.111. A solução proposta deve suportar a distribuição automatizada de patches e atualizações para mais de 150 aplicações.

5.112. A solução proposta deve ter funcionalidade de suporte ao modo de teste de patch.

5.113. A solução proposta deve incluir campos dedicados que contenham informações sobre ‘Exploração encontrada para a vulnerabilidade’.

5.114. A solução proposta deve incluir campos dedicados que contenham informações sobre “Ameaça encontrada para a vulnerabilidade”.

5.115. A solução proposta deve permitir que o administrador restrinja a capacidade dos usuários do dispositivo de aplicar eles próprios as atualizações da Microsoft.

5.116. A solução proposta deve permitir ao administrador especificar quais atualizações podem ser instaladas pelos usuários.

5.117. A solução proposta deve permitir ao administrador visualizar uma lista de atualizações e patches não relacionados aos dispositivos clientes.

5.118. A solução proposta deve apoiar a implantação do sistema operacional.

5.119. A solução proposta deve suportar Wake-on LAN e UEFI.

5.120. A solução proposta deve ter funcionalidade integrada de compartilhamento remoto de área de trabalho. Todas as operações de arquivo executadas no endpoint remoto durante a sessão devem ser registradas no Management Server.

5.121. A solução proposta deve ser capaz de fornecer correções de vulnerabilidades aos computadores clientes sem instalar as atualizações.

5.122. A solução proposta deve permitir que o administrador escolha as atualizações do Windows a serem instaladas, após o que o usuário do dispositivo cliente poderá instalar apenas as atualizações permitidas/selecionadas pelo administrador.

5.123. A solução proposta deve informar o administrador sobre atualizações e patches não relacionados no dispositivo cliente.

5.124. A solução proposta deve ser configurável/atribuível como fonte de atualização para atualizações da Microsoft e de terceiros.

5.125. A solução proposta deve permitir ao administrador selecionar o produto Microsoft e os idiomas para os quais as atualizações serão baixadas.

5.126. A solução proposta deve ser capaz de enviar/implantar remotamente arquivos EXE, MSI,

bat, cmd, MSP e permitir que o administrador defina o parâmetro de linha de comando para a instalação remota.

5.127. A solução proposta deve ser capaz de desinstalar aplicativos remotamente, não se limitando a programas antivírus incompatíveis.

5.128. A solução proposta deve permitir ao administrador utilizar uma única tarefa/trabalho e definir diferentes regras ou critérios de correção de vulnerabilidades para atualizações de aplicações da Microsoft e de terceiros.

5.129. A solução proposta deve permitir que o administrador configure regras para instalação de patches/atualizações da Microsoft e de terceiros:

5.129.1. Inicie a instalação ao reiniciar ou desligar o computador;

5.129.2. Instale o gerador necessário todos os pré-requisitos do sistema.

5.130. Permitir a instalação de novas versões de aplicativos durante as atualizações:

5.131. Baixe atualizações para o dispositivo sem instalá-las.

5.132. A solução proposta deve ter a capacidade de testar a instalação de atualizações em uma porcentagem de computadores antes de aplicá-la a todos os computadores de destino. O administrador deve ser capaz de configurar o número de computadores de teste como uma porcentagem e o tempo alocado antes da implementação completa em termos de horas.

5.133. A solução proposta deve permitir a remoção/desinstalação de atualizações específicas de aplicativos e sistemas operacionais.

5.134. O servidor de gerenciamento da solução proposta deve ser capaz de enviar logs para servidores SIEMs e SYSLOG nos seguintes formatos:

5.134.1. CEF;

5.134.2. LEEF.

5.135. A solução proposta deve ser capaz de rastrear licenças de aplicações de terceiros e gerar notificações de quaisquer violações potenciais.

5.136. O relatório da solução proposta deve conter informações CVE.

5.137. A solução proposta deve suportar instalação de aplicações e software de terceiros.

5.3. **Do módulo de gerenciamento simplificado**

5.3.1. A solução proposta deve suportar arquiteruta cloud.

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

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

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

5.3.5. 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.

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

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

5.3.8. A solução proposta deve incluir informações do endpoint:

5.3.8.1 IP público de internet;

5.3.8.2 IP interno do dispositivo;

5.3.8.3 Versão do agente de proteção;

5.3.8.4 Ultima comunicação com a console, contendo data e hora;

5.3.8.5 Informações do sistema operacional.

5.3.9. A solução proposta deve permitir proteger as caixas de correio do Exchange Online, os utilizadores do OneDrive e os sites do SharePoint Online geridos através do Office 365.

5.3.10. A solução proposta deve permitir detectar informações críticas em arquivos localizados nos armazenamentos em nuvem do Office 365.

5.3.11. A solução proposta deve incluir treinamento em segurança cibernética.

5.3.12. Requisitos gerais

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

5.3.13.1 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.

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

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

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

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

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

5.3.18.1 Proteção contra ameaças sem arquivos (Fileless);

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

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

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

5.3.21 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.

5.3.22 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.

5.3.23 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.

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

5.3.25 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.

5.3.26 A solução proposta deve incluir os seguintes componentes no sensor instalado no

endpoint:

5.3.26.1 Controles de aplicativos;
5.3.26.2 Controle web e dispositivos;
5.3.26.3 HIPS e Firewall;
5.3.26.4 Descoberta de patches e vulnerabilidades de sistemas operacionais Windows;
5.3.26.5 Gerenciamento de criptografia de arquivos e discos;
5.3.26.6 Controle adaptativo para detecção de anomalias.

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

5.3.28 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.

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

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

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

5.3.31.1 Bloqueio de aplicativos com base em sua categorização;
5.3.31.2 Bloqueio/permissão de pacotes, protocolos, endereços IP, portas e direção de tráfego específicos;
5.3.31.3 A adição de sub-redes e a modificação de permissões de atividade.

5.3.32 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:

5.3.32.1 A solução proposta deve ser capaz de bloquear ataques à rede e reportar a origem da infecção;
5.3.32.2 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.

5.3.33 A solução proposta deve incluir limpeza remota dos dispositivos com as seguintes funcionalidades:

5.3.33.1 Modo silencioso;
5.3.33.2 Discos rígidos e dispositivos removíveis;
5.3.33.3 De todos as contas de usuários do dispositivo.

5.3.34 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes modos:

5.3.34.1 Exclusão imediata de dados;
5.3.34.2 Exclusão de dados adiada.

5.3.35 A funcionalidade de limpeza remota de dados da solução proposta deve suportar os seguintes métodos de exclusão de dados:

5.3.35.1 Excluir usando os recursos do sistema operacional - os arquivos são excluídos;
5.3.35.2 Excluir completamente, sem recuperação - tornando praticamente impossível restaurar os dados após a exclusão.

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

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

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

5.3.39 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.

5.3.40 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.

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

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

5.3.43 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;

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

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

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

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

5.3.48 A solução proposta deve ser capaz de monitorar e bloquear ações que não são típicas dos computadores da rede de uma empresa.

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

5.3.50 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.

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

5.3.52 A solução proposta deve ser capaz de bloquear o uso de dispositivos de armazenamento USB ou permitir o acesso apenas aos dispositivos permitidos.

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

5.3.54 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.

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

5.3.56 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;

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

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

5.3.59 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.

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

5.3.61 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.

5.3.62 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.

5.3.63 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.

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

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

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

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

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

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

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

5.3.71 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.

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

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

5.3.73.1 Filtro de anexos.

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

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

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

5.3.76 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.).

5.3.77 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.

5.3.78 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.

5.3.79 A solução proposta deve incluir suporte ao protocolo IPv6.

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

5.3.81 A solução proposta deve incorporar a tecnologia de autoproteção de aplicação.

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

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

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

5.3.85 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.

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

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

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

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

5.3.90 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.

5.3.91 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.

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

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

5.3.94 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.

5.3.95 A solução proposta deve suportar endereços IPv6.

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

5.3.97 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.

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

5.3.99 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.

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

5.3.101 A solução proposta deve permitir a atualização automática do sensor de endpoint e de bases de dados de anti-malware.

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

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

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

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

5.3.106 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.

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

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

5.3.109 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.

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

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

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

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

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

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

5.3.116 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.

5.3.117 Os relatórios da solução proposta devem incluir informações sobre cada ameaça e a

tecnologia que a detectou.

5.3.118 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.

5.3.119 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.

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

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

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

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

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

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

5.3.124 Do modulo de gerenciamento de dispositivos móveis

5.3.125 O modulo deve ser integrado a console de gerenciamento.

5.3.126 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis, incluindo Android, Android 5.0 ou posterior (incluindo Android 12L, excluindo Go Edition).

5.3.127 A solução proposta deverá ser capaz de proteger ou gerenciar dispositivos móveis iOS, iOS 10–17 ou iPadOS 13–17.

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

5.3.129 A solução proposta deve suportar dispositivos iOS supervisionados.

5.3.130 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.

5.3.131 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.

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

5.3.133 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).

5.3.134 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.

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

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

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

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

5.3.138.1 Dados em contêineres;
5.3.138.2 Contas de e-mail corporativo;
5.3.138.3 Configurações para conexão à rede Wi-Fi corporativa e VPN;
5.3.138.4 Nome do ponto de acesso (APN);
5.3.138.5 Perfil do Android for Work;
5.3.138.6 Recipiente KNOX;
5.3.138.7 Chave do gerenciador de licença KNOX.

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

5.3.139.1 Todos os perfis de configuração instalados;
5.3.139.2 Todos os perfis de provisionamento;
5.3.139.3 O perfil iOS MDM.

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

5.3.141 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.

5.3.142 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:

5.3.142.1 Critérios de verificação do dispositivo;
5.3.142.2 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.

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

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

5.3.144.1 Cartões de memória e outras unidades removíveis;
5.3.144.2 Câmera do dispositivo;
5.3.144.3 Conexões Wi-Fi;
5.3.144.4 Conexões Bluetooth;
5.3.144.5 Porta de conexão infravermelha;
5.3.144.6 Ativação do ponto de acesso Wi-Fi;
5.3.144.7 Conexão de área de trabalho remota;
5.3.144.8 Sincronização de área de trabalho;
5.3.144.9 Definir configurações da caixa de correio do Exchange;
5.3.144.10 Configurar caixa de e-mail em dispositivos iOS MDM;
5.3.144.11 Configure contêineres Samsung KNOX;
5.3.144.12 Definir as configurações do perfil do Android for Work;

5.3.144.13 Configurar e-mail/calendário/contatos;
5.3.144.14 Defina as configurações de restrição de conteúdo de mídia;
5.3.144.15 Definir configurações de proxy no dispositivo móvel;
5.3.144.16 Configurar certificados e SCEP.

5.3.145 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.

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

5.3.146.1 Google Play, Huawei App Gallery e Apple App Store;
5.3.146.2 Portal de inscrição móvel KNOX;
5.3.146.3 Pacotes de instalação pré-configurados independentes.

5.3.147 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.

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

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

5.3.149.1 VMware AirWatch 9.3 ou posterior;
5.3.149.2 MobileIron 10.0 ou posterior;
5.3.149.3 IBM MaaS360 10.68 ou posterior;
5.3.149.4 Microsoft Intune 1908 ou posterior;
5.3.149.5 SOTI MobiControl 14.1.4 (1693) ou posterior.

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

5.3.151 A solução proposta deve suportar a implantação de sensor de endpoint iniciada pelo usuário através de:

5.3.151.1 Google Play;
5.3.151.2 Galeria de aplicativos Huawei;
5.3.151.3 Loja de aplicativos da Apple.

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

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

5.3.154 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.

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

5.3.156 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.

5.3.157 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.

5.3.158 A solução proposta deve ser capaz de gerenciar e monitorar dispositivos móveis a

partir do mesmo console usado para gerenciar computadores e servidores.

5.3.159 A solução proposta deve fornecer funcionalidade Anti-Roubo, para que dispositivos perdidos e/ou deslocados possam ser localizados, bloqueados e apagados remotamente.

5.3.160 A solução proposta deve fornecer a possibilidade de bloquear o lançamento de aplicativos proibidos no dispositivo móvel.

5.3.161 A solução proposta deve ser capaz de impor configurações de segurança, como restrições de senha e criptografia, em dispositivos móveis.

5.3.162 A solução proposta deve ter a capacidade de enviar aplicações recomendadas/exigidas pelo administrador para o dispositivo móvel.

5.3.163 A solução proposta deverá possuir Controle de Aplicativos com os modos de aplicação Proibido/Permitido.

5.3.164 A solução proposta deve incluir um modelo de assinatura integrado a nuvem do fabricante para proteção de ataques mais recentes;

5.3.165 A solução proposta deve proteger contra ameaças online em dispositivos iOS.

5.4 Do módulo de EDR

5.4.18 Deve apresentar um gráfico de propagação de ameaças com os principais processos. conexões de rede, DLLs, seções de registro afetado ou envolvido no alerta.

5.4.19 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.

5.4.20 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.

5.4.21 Dever ser integrado ao portal de inteligência do fornecedor para enriquecimento dos detalhes da análise.

5.4.22 Deve apresentar informações detalhadas contendo.

5.4.23 Usuário que executou a ação.

5.4.24 Informações acesso privilegiado.

5.4.25 A solução proposta deve ter sandbox em nuvem do fabricante integrada para verificar automaticamente arquivos e aplicar respostas caso atividades suspeitas sejam detectadas.

5.4.26 A solução proposta deve suportar integração com serviço de reputação em nuvem.

5.4.27 A solução proposta deve oferecer suporte ao gerenciamento central e à análise por meio do console Web local e do console de gerenciamento em nuvem avançado. (Dados relacionados ao incidente, status do sistema e dados de verificação de integridade, configurações, etc.).

5.4.28 O agente EDR deve ter integração com o aplicativo de proteção de endpoint(agente único).

5.4.29 Soluções EDR e proteção de endpoint devem ter console unificado para administradores e analistas.

5.4.30 A solução proposta deve suportar a detecção automatizada de atividades maliciosas usando a solução Endpoint Protection e a tecnologia de sandbox na nuvem.

5.4.31 A solução proposta deve complementar as informações do veredicto da solução

Endpoint Protection com artefatos do sistema sobre a detecção.

5.4.32 A solução proposta deve suportar a geração automática de indicadores de ameaça (IoC) após a detecção ocorrer com capacidade de aplicar ações de resposta.

5.4.33 A solução deve ter a capacidade de forçar a execução da varredura IoC em todos os endpoints com agentes EDR instalados.

5.4.34 A solução proposta deve suportar a execução de varredura IoC de acordo com um agendador.

5.4.35 A solução proposta deve suportar a importação de IoC de terceiros no formato OpenIoC para uso em digitalização em rede.

5.4.36 A solução proposta deve oferecer suporte à verificação usando conjuntos de IoCs gerados automaticamente, carregados ou externos (de terceiros) para detectar ameaças anteriores não detectadas.

5.4.37 A solução proposta deve permitir suportar a exportação do IoC gerado pela solução para monitorar vulnerabilidades existentes nos dispositivos gerenciados, um arquivo no formato OpenIoC.

5.4.38 A solução proposta deve gerar um cartão de incidente detalhado relacionado à ameaça detectada em um endpoint.

5.4.39 A solução proposta deve permitir detectar e erradicar ataques avançados, realizar análises de causa raiz com um cartão de incidente visualizado. Um cartão de incidente deve incluir pelo menos as seguintes informações sobre a ameaça detectada:

5.4.40 Gráfico da cadeia de desenvolvimento de ameaças e detalhamento para análise posterior (cadeia de ataque).

5.4.41 Informações sobre o dispositivo no qual a ameaça foi detectada, contendo: nome, endereço IP, endereço MAC, lista de usuários, sistema operacional.

5.4.42 Informações gerais sobre a detecção, incluindo modo de detecção.

5.4.43 Alterações no registro associadas à detecção.

5.4.44 Histórico da presença de arquivos no dispositivo.

5.4.45 Ações de resposta executadas pela aplicação.

5.4.46 O gráfico da cadeia de desenvolvimento de ameaças (kill chain) deve fornecer informações visuais sobre os objetos envolvidos no incidente, por exemplo, sobre os principais processos no dispositivo, conexões de rede, bibliotecas, registro, etc.

5.4.47 A visualização de incidente deve apresentar uma visão detalhada dos artefatos do sistema e dos dados relacionados ao incidente para análise da causa raiz:

5.4.47.1 Processo;
5.4.47.2 Conexões de rede;
5.4.47.3 Alterações no registro;
5.4.47.4 Detalhes do download de objeto.

5.4.48 A solução proposta deve fornecer orientação de resposta (resposta guiada).

5.4.49 A solução proposta deve suportar “clique único” no console de gerenciamento avançado para resposta a um incidente.

5.4.50 A solução proposta deve suportar pelo menos as seguintes ações de resposta que um administrador pode executar quando ameaças são detectadas:

5.4.50.1 Impedir a execução de objetos;
5.4.50.2 Isolamento de host;

5.4.50.3 Excluir objeto do host ou grupo de hosts;
5.4.50.4 Encerrar um processo no dispositivo;
5.4.50.5 Colocar um objeto em quarentena;
5.4.50.6 Execute a verificação do sistema;
5.4.50.7 Execução remota de programa/processo/comando;
5.4.50.8 Iniciar a varredura IoC para um grupo de hosts.

6. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE

6.1. A Alesc possui um parque tecnológico com aproximadamente 1.100 (um mil e cem) computadores, entre servidores e estações de trabalho (máquinas físicas e virtuais). Toda essa estrutura tecnológica é alvo de constantes ataques maliciosos, que buscam causar o caos administrativo por meio dos mais variados mecanismos, corromper arquivos de trabalho diário, roubar informações privilegiadas ou danificar estruturas de tecnologia, o que pode gerar um enorme prejuízo, inclusive financeiro.

6.2. Com a aquisição de uma solução avançada de proteção, nossa organização passará a contar com uma segurança ainda mais abrangente. Atualmente, nossa rede não dispõe de um sistema antispam, o que nos torna vulneráveis a mensagens indesejadas e ataques de phishing. Com esse upgrade, será implementada uma solução específica para plataformas de colaboração e produtividade, incluindo robustos mecanismos de antispam que garantirão maior segurança para nossos e-mails e comunicações. A proteção também se estende a serviços essenciais, como OneDrive, SharePoint e outros aplicativos do ecossistema Microsoft. Essa integração proporcionará maior proteção para nossos dados e sistemas.

6.3. As corporações que fazem uso ou oferecem serviços por meio da Internet devem ter extrema preocupação com esse canal de comunicação, que apesar do benefício incontestável de permitir conectividade em âmbito global, também representa, em contrapartida, risco potencial de segurança à informação trocada entre os usuários.

6.4. Para que seja possível manter adequado nível de segurança nesse ambiente e assim preservar os ativos corporativos (hardware, software e dados), garantindo a integridade, confidencialidade e segurança das informações institucionais, torna-se imprescindível a adoção de soluções que minimizem os riscos e evitem prejuízos, não só em relação às questões que envolvem tecnologia, mas também de ordem financeira e da imagem institucional.

6.5. Nesse sentido, a contratação da solução completa e integrada de segurança é importante para garantir as melhores práticas de Segurança da Informação em conformidade com as normas de referência dessa área.

6.6. A solução atual, contratada por meio do Contrato nº 261/2021 que tem seu vencimento em 09/05/2025, denominada internamente "antivírus corporativo", provê proteção constantemente atualizada contra grande parte das infecções existentes na Internet ou em arquivos trazidos pelos usuários de fora de nossa rede. A proteção contempla:

a) Estações de trabalho: cada estação de trabalho (computador de mesa ou notebook) possui um antivírus instalado e atualizado constantemente;

b) Servidores de rede: cada servidor possui um antivírus instalado e atualizado constantemente;

c) Navegação Web: todos os computadores da Alesc, quando navegam na Internet, passam por um sistema que faz a proteção e triagem do conteúdo acessado, minimizando a contaminação dos computadores da Alesc.

6.7. Todos estes componentes são gerenciados por um sistema central, denominado SERVIDOR DE ADMINISTRAÇÃO E CONSOLE ADMINISTRATIVA. Este sistema coordena os esforços no sentido de manter toda a estrutura de segurança atualizada e operacional.

6.8. A forte integração entre as ferramentas de segurança permite que um evento malicioso

detectado no dispositivo de um usuário final (endpoint) possa ser prontamente bloqueado antes de alcançar a rede interna por ativos de proteção de perímetro. Para isso, é importante que os eventos possam ser automaticamente detectados e correlacionados, o que normalmente só é possível com ferramentas de um mesmo fabricante, permitindo um bloqueio coordenador e eficaz do evento.

6.9. Sendo assim, é indiscutível a necessidade de se manter o uso deste tipo de solução, para proteção das estações de trabalho, equipamentos servidores de rede, navegação na Internet e correio eletrônico, sendo que a manutenção da solução existente é a mais vantajosa conforme exposto a seguir.

7. REQUISITOS DA CONTRATAÇÃO

7.1. É vedada a subcontratação do objeto do contrato.

7.2. A participação de empresas em consórcios é recomendável quando o objeto da contratação possui porte elevado, alta complexidade ou exige múltiplas especialidades de seu executor, de forma que a competitividade da licitação poderia ser afetada pela escassez de empresas aptas, individualmente, a atender aos requisitos do edital. No entanto, considerando que a presente contratação não apresenta essas características, não será permitida a participação de consórcios de empresas nesta licitação.

7.3. Na presente contratação não haverá a participação de cooperativas, pois a execução dos serviços demanda subordinação dos trabalhadores em relação à pessoa jurídica contratada pela Administração.

7.4. SUPORTE TÉCNICO

7.4.1. A CONTRATADA deverá prestar suporte técnico para toda a solução instalada, em regime 12x5 (12 horas por dia, cinco dias por semana) através de e-mail, internet, telefone e no endereço da CONTRATANTE.

7.4.2. A CONTRATADA deverá possuir profissional técnico treinado ou certificado pelo fabricante, sendo comprovado através de Certificado emitido e assinado pelo Fabricante.

7.5. Qualificação técnica:

7.5.1. A empresa deverá ser certificada como revenda oficial da marca oferecida, comprovando através de carta do fabricante especificamente para este Edital.

8. MODELO DE EXECUÇÃO DO OBJETO (FORMA, PRAZO E LOCAL DE ENTREGA)

8.1. A Contratada deverá iniciar os serviços em até 30 (trinta) dias após a assinatura do contrato.

8.2. Antes de findar o prazo estabelecido no subitem, a Contratada poderá formalizar pedido de prorrogação, cujas razões expostas serão examinadas pela Contratante, que decidirá pela prorrogação ou não do prazo ou aplicação das penalidades previstas no contrato.

8.3. A visita técnica para implementação do serviço deverá ocorrer Gerência de Segurança e Administração de Redes na Unidade Administrativa da Assembleia Legislativa do Estado de Santa Catarina, localizada na Avenida Mauro Ramos, nº 300, Centro, Florianópolis/SC, de segunda a sexta-feira das 13h às 19h.

8.4. As licenças a serem fornecidas pela Contratada deverão ser enviadas para o e-mail da Gerência de Segurança e Administração de Redes, no seguinte endereço eletrônico: redes@alesc.sc.gov.br.

8.5. Após a entrega, será realizada uma avaliação e homologação pelo(s) responsável(is) técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do

fabricante.

9. MODELO DE GESTÃO DO CONTRATO

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

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

9.3. As comunicações entre a Alesc e a Contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

9.4. A Alesc poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

9.5. O gestor e fiscais do contrato serão designados mediante Portaria do Diretor-Geral da Assembleia Legislativa, no Diário da Alesc e deverão se ater aos ditames do Ato de Mesa nº. 317, de 19 de novembro de 2020, que dispõe sobre a gestão e fiscalização dos contratos administrativos no âmbito da Alesc.

10. OBRIGAÇÕES DA CONTRATANTE

10.1. Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com o contrato e seus anexos;

10.2. Receber o objeto no prazo e condições estabelecidas neste Termo de Referência;

10.3. Notificar a contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

10.4. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela contratada.

10.5. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133/2021.

10.6. Efetuar o pagamento à Contratada do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

10.7. Aplicar à Contratada as sanções previstas na lei e neste Contrato.

10.8. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

10.9. Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pela contratada no prazo máximo de 1 (um) mês, admitida a prorrogação motivada por igual período.

10.10. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

11. OBRIGAÇÕES DA CONTRATADA

11.1. A Contratada deve cumprir todas as obrigações constantes deste Termo de Referência, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

11.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.

11.3. Alocar os empregados necessários ao perfeito cumprimento das cláusulas do contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

11.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

11.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo Contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos.

11.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133/2021.

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

11.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

11.9. Prestar todo esclarecimento ou informação solicitada pelo Contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

11.10. Paralisar, por determinação do Contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

11.11. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

11.12. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

11.13. Submeter previamente, por escrito, ao Contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

11.14. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

11.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.

11.16. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação.

11.17. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato;

11.18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133/2021.

11.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do Contratante;

12. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

12.1. A contratação do serviço de antivírus será estruturada em duas modalidades de pagamento distintas: um pagamento único referente à aquisição das licenças necessárias para utilização da solução e um pagamento mensal, ao longo de 36 meses, para a prestação do suporte técnico especializado.

12.2. O pagamento se dará por meio de crédito bancário em conta corrente identificada pela contratada, mediante apresentação do documento fiscal, após a realização dos serviços devidamente atestados pelo fiscal do contrato e com aceite do Fiscal e do Gestor do contrato, no prazo de 30 (trinta) dias a partir da data de aceite do documento fiscal.

12.3. No caso do não pagamento do documento fiscal até o 30º (trigésimo) dia da data de aceite, por culpa exclusiva do Contratante, será efetuada a atualização monetária do 31º (trigésimo primeiro) dia até a data da efetiva quitação, atualizando-se o valor com base nos mesmos critérios adotados para a atualização das obrigações tributárias, em observância ao que dispõe o art. 117 da Constituição Estadual.

12.4. O credor que não possuir conta corrente na instituição financeira contratada pela Alesc (Banco do Brasil) poderá receber o pagamento em outras instituições financeiras, por meio de crédito em conta corrente do favorecido, ficando, contudo, responsável pelo pagamento das tarifas bancárias derivadas da operação (nos termos do art. 9º, § 4º, do Decreto nº 1.073, de 23 de fevereiro de 2017).

12.5. Se, quando da efetivação do pagamento, os documentos que comprovem a regularidade fiscal e trabalhista estiverem com a validade expirada, o pagamento não ficará retido, devendo, entretanto, a contratada apresentar, no prazo máximo de até 30 (trinta) dias, novos documentos dentro do prazo de validade, sob pena de ser-lhe aplicada sanção, após defesa, por inadimplemento parcial do contrato.

12.6. Caso haja aplicação de multa/glosa, a contratada deverá emitir novo documento fiscal com o desconto correspondente ao valor da multa/glosa. Caso não seja emitido novo documento fiscal, o valor será descontado de qualquer fatura ou crédito existente na Alesc em favor da contratada, sendo a base de cálculo para retenção de IR o valor total do documento fiscal, conforme IN RFB nº 1234, de 11 de janeiro de 2012. Caso o valor da multa/glosa seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

12.7. Caberá à contratada emitir e apresentar os documentos fiscais correspondentes aos serviços objeto deste contrato, no início de cada mês subsequente àquele no qual os serviços foram realizados, expressas em moeda corrente, com a discriminação dos serviços efetivamente efetuados, inclusive com período de referência da prestação dos serviços, devidamente atestadas por servidor designado pela Alesc.

12.8. O código de atividade (CNAE) deverá ser compatível com o objeto deste contrato.

12.9. O número do contrato e os dados bancários deverão constar do documento fiscal.

12.10. Só serão autorizados, para efeito de pagamento, os documentos fiscais referentes a serviços autorizados, identificados e efetivamente realizados, até o período correspondente.

12.11. No pagamento deverão ser efetuadas as retenções e recolhimentos fiscais determinados pela legislação tributária.

12.12. Sendo identificada cobrança indevida ou outras irregularidades/divergências, os fatos serão informados à contratada, e a contagem do prazo para pagamento será reiniciada a partir da reapresentação da Nota Fiscal devidamente corrigida.

12.13. Sendo identificada cobrança indevida após o pagamento do documento fiscal, os fatos serão informados à contratada para que seja feita glosa do valor correspondente no próximo documento de cobrança.

12.14. O aceite dos serviços prestados por força desta contratação será feito mediante ateste dos documentos fiscais, correspondendo tão somente aos serviços efetivamente utilizados. Não serão pagos serviços não executados/autorizados.

12.15. A contratada deverá emitir a nota fiscal em observância às regras de retenção de tributos dispostas na Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012, bem como apresentar documentação comprobatória em caso de isenção ou imunidade.

13. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

13.1. O fornecedor será selecionado por meio da realização de procedimento de licitação, na modalidade Pregão, sob a forma eletrônica, com critério de julgamento pelo menor preço.

14. HABILITAÇÃO

14.1. A **habilitação jurídica, fiscal, social e trabalhista** será aquela padronizada no Edital de licitação.

14.2. Para fins **habilitação econômico-financeira** deverá ser apresentada a certidão negativa da falência expedida pelo distribuidor da sede do licitante.

14.3. A licitante deverá apresentar a seguinte documentação relativa à **qualificação técnica**:

14.3.1. Comprovação de aptidão para a prestação dos serviços compatíveis com o objeto desta contratação, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado.

14.3.1.1. O licitante deverá fornecer atestados que comprovem o fornecimento de ao menos 300 (trezentas) licenças.

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

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

14.3.2. Certificado que comprove que a Licitante é revendedora oficial da marca oferecida, comprovando através de carta do fabricante.

15. INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

15.1. Comete infração administrativa, nos termos da Lei nº 14.133/2021, a contratada que:

a) dar causa à inexecução parcial do contrato;

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

c) dar causa à inexecução total do contrato;

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

e) não manter a proposta, salvo em decorrência de fato superveniente devidamente justificado;

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

g) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo justificado;

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

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

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

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

l) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.14.2.

15.2. Serão aplicadas à Contratada que incorrer nas infrações acima descritas as seguintes sanções:

a) advertência, quando a contratada der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

b) impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c”, “d”, “e”, “f” e “g” do subitem anterior sempre que não se justificar a imposição de penalidade mais grave;

c) declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “h”, “i”, “j”, “k” e “l” do subitem anterior acima deste Contrato, bem como nas alíneas “b”, “c”, “d”, “e”, “f” e “g”, que justifiquem a imposição de penalidade mais grave.

d) Multa, conforme tabela a seguir:

Tipo	Correspondência	Evento
Moratória	0,5% (meio por cento) do valor total mensal do contrato, por dia de atraso	Não atendimento a qualquer prazo estabelecido, pelo descumprimento ou inobservância a qualquer item estabelecido em prazo para execução e implantação;
Compensatória	1% (um por cento) do valor total do contrato, por ocorrência	Descumprimento ou inobservância a qualquer item estabelecido em Especificações Técnicas,
Compensatória	5% (cinco por cento) do valor total do contrato.	Infração descrita na alínea “a” do subitem anterior
Compensatória	10% (dez por cento) do valor total do contrato.	Infração descrita na alínea “b” do subitem anterior

Compensatória	20% (vinte por cento) do valor total do contrato.	Infração descrita na alínea “c” do subitem anterior
Compensatória	10% (vinte por cento) do valor da proposta.	Infrações descritas nas alíneas “d”, “e” e “f” do subitem anterior
Compensatória	5% (cinco por cento) do valor do contrato.	Infração descrita na alínea “g” do subitem anterior
Compensatória	20% (vinte por cento) do valor total do contrato ou do valor estimado da contratação, quando for o caso.	Infrações descritas nos itens “h” a “l” do subitem anterior.
Compensatória	5% (cinco por cento) do valor total mensal do contrato.	Por indicador ou meta de nível de serviço, que tenha sido objeto de tentativa de burla, fraude, manipulação ou descaracterização pela Contratada.
Compensatória	2% (dois por cento) do valor total mensal do contrato	Por ocorrência que permaneça sem solução por mais de um período de faturamento consecutivo.

15.3. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

15.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao contratante.

15.5. Para os efeitos de aplicação das sanções acima descritas, considera-se como valor total do contrato o valor total da autorização de fornecimento ou documento equivalente.

15.6. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

15.7. A multa pode ser descontada da garantia, dos pagamentos devidos à Contratada em razão do contrato em que houve a aplicação da multa ou de eventual outro contrato havido entre a Alesc e a Contratada.

15.8. Além das disposições previstas na Lei nº 14.133/2021, o processo de aplicação de sanções contratuais seguirá o disposto no Ato da Mesa nº 257/2024.

15.9. A Meta de Atendimento e suporte será conforme tabela a seguir, limitada a 10%:

Atividade	**Nível Mínimo Serviço**	**Indicador Meta**	**Indicador**	**Glosa**
Gerenciamento de regras	120 minutos após abertura do chamado	120 minutos	Regra implementada	2%
Alteração de configurações	240 minutos após abertura do chamado	240 minutos	Configuração implementada	2%

Verificação de Logs	24 horas após abertura do chamado	24 horas	Arquivo de log enviado ao solicitante	5%
Atualização de plataformas, implantação de patches	5 dias após a liberação das atualizações pelo fabricante	5 dias	Patch e fix instalados	5%
Registro de incidentes de segurança pela contratada	15 minutos após o primeiro registro ou sintoma relacionado ao evento	15 minutos	Chamado aberto	2%
Início de atuação para resolução de incidentes de segurança	15 minutos após abertura de chamado pelo cliente ou pela contratada	15 minutos	Registro das ações tomadas no chamado pelo responsável pela resolução	2%
Resolução de incidentes que provoquem indisponibilidade	120 minutos	120 minutos	Chamado concluído	2%
Alteração de política de segurança	120 minutos após a abertura do chamado	120 minutos	Política implantada	2%
Resolução de incidentes que não provoquem indisponibilidade	240 minutos	240 minutos	Chamado concluído	2%
Atendimento de chamados para esclarecimento de dúvidas	24 horas após abertura do chamado pelo cliente	24 horas	Chamado concluído	5%
Realização periódica de scan de vulnerabilidades	Mensal	30 dias	Relatórios de vulnerabilidades apresentados	5%
Realização de implantação de patches de segurança de em ativos da rede	Mensal	30 dias	Relatórios de resultado da implantação	5%
Realização de scan sob demanda	24 horas após a abertura do chamado	24 horas	Relatórios de vulnerabilidades apresentados	2%

16. ADEQUAÇÃO ORÇAMENTÁRIA

16.1. As despesas pertinentes ao objeto do presente Edital serão informadas pela Coordenadoria de Execução Orçamentária.

17. QUADRO-RESUMO DO TERMO DE REFERÊNCIA

Modalidade	Pregão Eletrônico
Sistema de Registro de Preços	Não
Em caso de SRP, necessita termo de contrato?	Não se aplica
Critério de julgamento	Menor preço
Parcelamento	Não se aplica
Empresas em consórcio	Não permitido
Cooperativas	Não permitido
Habilitação Técnica	Sim
Habilitação econômico-financeira	Sim
Vistoria Técnica	Não
Amostra/Prova de Conceito	Não
Contrato continuado	Sim
Índice de Reajuste	IPCA

Equipe de Planejamento	
Elias Amaral dos Santos	Integrante Técnico
Leonardo Ulisses Moraes	Membro da Comissão de Planejamento

ANEXO II

EDITAL DE PREGÃO ELETRÔNICO Nº 005/2025

PLANILHA DE VALORES MÁXIMOS ADMISSÍVEIS

Item	Descrição	Unid.	Quantitativo	CATSER	Valor unitário	Subtotal (R$)
1	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT COM UPGRADE PARA A VERSÃO NEXT EDR OPTIMUM	UN.	1150.00	350949	123,09	141.553,50

2	SERVIÇO DE SUPORTE TÉCNICO INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO BÁSICO E ATENDIMENTO “ONLINE” E “ON SITE”	MÊS	36.00	350949	2.940,00	105.840,00
					Valor Máximo Admissível (R$):	247.393,50

ANEXO III

EDITAL DE PREGÃO ELETRÔNICO Nº 005/2025

MODELO DE PROPOSTA

NOME DA EMPRESA:
_____

ENDEREÇO: _____ CIDADE: _____ CEP: _____-___
ESTADO: ___

FONE DA EMPRESA: _____ FONE DO REPRESENTANTE:
_____

CNPJ Nº: _____

BANCO: _____ AGÊNCIA: _____ CONTA CORRENTE:
_____

E-MAIL: _____ RESPONSÁVEL PELA ASSINATURA DO CONTRATO:
_____

A presente proposta tem como objeto a aquisição dos itens ou contratação dos serviços abaixo discriminados, em conformidade com as especificações, quantidades e demais condições definidas no edital e seus anexos.

Item	Descrição	Unid.	Quant.	Valor unitário	Subtotal

Valor total	

I. A presente proposta tem validade de 60 (sessenta) dias;

II. Declaro que cumpro e acato todos os dispositivos estabelecidos no edital e seus anexos.

III. Declaro que a presente proposta 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 presente data.

Florianópolis/SC, ____ de _____ de 2024.

Representante legal

(Assinatura e carimbo da empresa)

ANEXO IV

EDITAL DE PREGÃO ELETRÔNICO Nº 005/2025

MINUTA DO CONTRATO

CONTRATO N° XXX/2025

Contratação de empresa especializada para o fornecimento de licenças Kaspersky Endpoint Security for Business Select, com Upgrade para a versão NEXT EDR OPTIMUM, que entre si firmam a Assembleia Legislativa do Estado de Santa Catarina e a empresa XXXXXXX, mediante cláusulas e condições a seguir:

CONTRATANTE: Assembleia Legislativa do Estado de Santa Catarina, inscrita no CNPJ sob o n° 83.599.191/0001-87, com sede na Rua Doutor Jorge Luz Fontes n° 310, Centro, Florianópolis/SC, CEP 88020-900, telefone (48) 3221-2512, e-mail dti@alesc.sc.gov.br, representada neste ato por seu Diretor-Geral, Leonardo Lorenzetti, e por seu Diretor de Tecnologia e Informações, Brian Venceslau Michalski.

CONTRATADA: Xxxxxx Xxxxx, inscrita no CNPJ sob XXXXXXX, com sede na XxxxxxxXxxx, telefone (XX) XXXX-XXXX, e-mail xxxxxxx, representada neste ato por Xxxxxxx, inscrita(o) no CPF sob o n° XXX

FUNDAMENTO LEGAL

· Lei Federal nº 14.133, de 1º de abril de 2021;
· Lei Complementar nº 123, de 14 de dezembro de 2006;
· Atos da Mesa nº 149, de 30 de abril de 2020, nº 195, de 16 de junho de 2020, e nº 257, de 28 de maio de 2024;
· Pregão Eletrônico nº 005/2025; e
· Processo SEI n° 24.0.000044917-9.

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de empresa especializada para o fornecimento de licenças *Kaspersky Endpoint Security for Business Select*, com Upgrade para a versão NEXT EDR OPTIMUM, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	UNIDADE	QUANTIDADE	VALOR UNITÁRIO (R$)	VALOR TOTAL (R$)
1	KASPERSKY ENDPOINT SECURITY FOR BUSINESS SELECT COM UPGRADE PARA A VERSÃO NEXT EDR OPTIMUM	UN.	1150.00		
2	SERVIÇO DE SUPORTE TÉCNICO INCLUINDO INSTALAÇÃO, CONFIGURAÇÃO, TREINAMENTO BÁSICO E ATENDIMENTO “ONLINE” E “ON SITE”	MÊS	36.00		
				Valor Máximo Admissível (R$):	

1.3. Vinculam esta contratação, independentemente de transcrição:

1.3.1. O Termo de Referência;

1.3.2. O Edital da Licitação;

1.3.3. A Proposta da contratada;

1.3.4. Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação é de 36 (trinta e seis) meses contados da assinatura do contrato, prorrogável na forma do artigo 107 da Lei n° 14.133, de 2021, respeitada a vigência máxima decenal.

2.2. A prorrogação de que trata este item é condicionada ao ateste, pela autoridade competente, de que as condições e os preços permanecem vantajosos para a Administração, permitida a negociação com a contratada.

2.3. A contratada não tem direito subjetivo à prorrogação contratual.

2.4. A prorrogação de contrato deverá ser promovida mediante celebração de termo aditivo.

2.5. Nas eventuais prorrogações contratuais, os custos não renováveis já pagos ou amortizados ao longo do primeiro período de vigência da contratação deverão ser reduzidos ou eliminados como condição para a renovação.

2.6. O contrato não poderá ser prorrogado quando a contratada tiver sido penalizada nas sanções de declaração de inidoneidade ou impedimento de licitar e contratar com poder público, observadas as abrangências de aplicação.

CLÁUSULA TERCEIRA – MODELO DE EXECUÇÃO DO OBJETO

3.1. A Contratada deverá iniciar os serviços em até 30 (trinta) dias após a assinatura do contrato.

3.2. Antes de findar o prazo estabelecido no subitem, a Contratada poderá formalizar pedido de prorrogação, cujas razões expostas serão examinadas pela Contratante, que decidirá pela prorrogação ou não do prazo ou aplicação das penalidades previstas no contrato.

3.3. A visita técnica para implementação do serviço deverá ocorrer Gerência de Segurança e Administração de Redes na Unidade Administrativa da Assembleia Legislativa do Estado de Santa Catarina, localizada na Avenida Mauro Ramos, nº 300, Centro, Florianópolis/SC, de segunda a sexta-feira das 13h às 19h.

3.4. As licenças a serem fornecidas pela Contratada deverão ser enviadas para o e-mail da Gerência de Segurança e Administração de Redes, no seguinte endereço eletrônico: redes@alesc.sc.gov.br.

3.5. Após a entrega, será realizada uma avaliação e homologação pelo(s) responsável(is) técnicos. A análise para comprovação das características técnicas consistirá em avaliar as documentações apresentadas e também informações de registro das licenças no site oficial do fabricante.

CLÁUSULA QUARTA – MODELO DE GESTÃO DO CONTRATO

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

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

4.3. As comunicações entre a Alesc e a Contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.

4.4. A Alesc poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

4.5. O gestor e fiscais do contrato serão designados mediante Portaria do Diretor-Geral da Assembleia Legislativa, no Diário da Alesc e deverão se ater aos ditames do Ato de Mesa nº. 317,

de 19 de novembro de 2020, que dispõe sobre a gestão e fiscalização dos contratos administrativos no âmbito da Alesc.

CLÁUSULA QUINTA – SUBCONTRATAÇÃO

5.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA SEXTA – PREÇO

6.1. O valor total da contratação é de R$..... (.....).

6.2. No valor acima estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais, trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

6.3. O valor acima é meramente estimativo, sendo que será uma parcela única referente à aquisição das licenças e um pagamento mensal, ao longo de 36 meses, para a prestação do suporte técnico especializado**,** de forma que os pagamentos devidos à contratada dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA SÉTIMA – PAGAMENTO

7.1. A contratação do serviço de antivírus será estruturada em duas modalidades de pagamento distintas: um pagamento único referente à aquisição das licenças necessárias para utilização da solução e um pagamento mensal, ao longo de 36 meses, para a prestação do suporte técnico especializado.

7.2. O pagamento se dará por meio de crédito bancário em conta corrente identificada pela contratada, mediante apresentação do documento fiscal, após a realização dos serviços devidamente atestados pelo fiscal do contrato e com aceite do Fiscal e do Gestor do contrato, no prazo de 30 (trinta) dias a partir da data de aceite do documento fiscal.

7.3. No caso do não pagamento do documento fiscal até o 30º (trigésimo) dia da data de aceite, por culpa exclusiva do CONTRATANTE, será efetuada a atualização monetária do 31º (trigésimo primeiro) dia até a data da efetiva quitação, atualizando-se o valor com base nos mesmos critérios adotados para a atualização das obrigações tributárias, em observância ao que dispõe o art. 117 da Constituição Estadual.

7.4. O credor que não possuir conta corrente na instituição financeira contratada pela Alesc (Banco do Brasil) poderá receber o pagamento em outras instituições financeiras, por meio de crédito em conta corrente do favorecido, ficando, contudo, responsável pelo pagamento das tarifas bancárias derivadas da operação (nos termos do art. 9º, § 4º, do Decreto nº 1.073, de 23 de fevereiro de 2017).

7.5. Se, quando da efetivação do pagamento, os documentos que comprovem a regularidade fiscal e trabalhista estiverem com a validade expirada, o pagamento não ficará retido, devendo, entretanto, a contratada apresentar, no prazo máximo de até 30 (trinta) dias, novos documentos dentro do prazo de validade, sob pena de ser-lhe aplicada sanção, após defesa, por inadimplemento parcial do contrato.

7.6. Caso haja aplicação de multa/glosa, a contratada deverá emitir novo documento fiscal com o desconto correspondente ao valor da multa/glosa. Caso não seja emitido novo documento fiscal, o valor será descontado de qualquer fatura ou crédito existente na Alesc em favor da contratada, sendo a base de cálculo para retenção de IR o valor total do documento fiscal, conforme IN RFB nº 1234, de 11 de janeiro de 2012. Caso o valor da multa/glosa seja superior ao crédito eventualmente existente, a diferença será cobrada administrativamente ou judicialmente, se necessário.

7.7. Caberá à contratada emitir e apresentar os documentos fiscais correspondentes aos serviços objeto deste contrato, no início de cada mês subsequente àquele no qual os serviços foram

realizados, expressos em moeda corrente, com a discriminação dos serviços efetivamente efetuados, inclusive com período de referência da prestação dos serviços, devidamente atestadas por servidor designado pela Alesc.

7.7.1. O código de atividade (CNAE) deverá ser compatível com o objeto deste contrato.

7.7.2. O número do contrato e os dados bancários deverão constar do documento fiscal.

7.8. Só serão autorizados, para efeito de pagamento, os documentos fiscais referentes a serviços autorizados, identificados e efetivamente realizados, até o período correspondente.

7.9. No pagamento deverão ser efetuadas as retenções e recolhimentos fiscais determinados pela legislação tributária.

7.10. Sendo identificada cobrança indevida ou outras irregularidades/divergências, os fatos serão informados à contratada, e a contagem do prazo para pagamento será reiniciada a partir da reapresentação da Nota Fiscal devidamente corrigida.

7.11. Sendo identificada cobrança indevida após o pagamento do documento fiscal, os fatos serão informados à contratada para que seja feita glosa do valor correspondente no próximo documento de cobrança.

7.12. O aceite dos serviços prestados por força desta contratação será feito mediante ateste dos documentos fiscais, correspondendo tão somente aos serviços efetivamente utilizados. Não serão pagos serviços não executados/autorizados.

7.13. A contratada deverá emitir a nota fiscal em observância às regras de retenção de tributos dispostas na Instrução Normativa RFB nº 1.234, de 11 de janeiro de 2012, bem como apresentar documentação comprobatória em caso de isenção ou imunidade.

7.14. Caso a contratada se enquadre e opte pela desoneração da folha de pagamento, disciplinada pela Lei nº 12.546, de 14 de dezembro de 2011, deverá informar essa opção no corpo da nota fiscal, bem como apresentar a declaração do Anexo III da IN RFB nº 2053/2021 devidamente preenchida e assinada

CLÁUSULA OITAVA – REAJUSTE

8.1. Após o interregno de um ano, por meio de pedido da contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice Nacional de Preços ao Consumidor Amplo – IPCA.

8.2. O índice a ser aplicado será referente a 12 (doze) meses, contados a partir do dia 04/04/2025, data da consolidação da Pesquisa de Preços.

8.3. O reajuste será concedido após transcorrer 12 (doze) meses da vigência do contrato.

8.4. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.

8.5. No caso de atraso ou não divulgação do índice de reajustamento, o contratante pagará à contratada a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja divulgado o índice definitivo.

8.6. Nas aferições finais, o índice utilizado para reajuste será, obrigatoriamente, o definitivo.

8.7. O reajuste será realizado por apostilamento ou por termo aditivo.

8.8. Sob pena de preclusão, o direito ao reajuste deverá ser pleiteado pela Contratada antes:

8.8.1. da data de cada aniversário do contrato;

8.8.2. do encerramento do contrato.

8.9. Não haverá reajuste de preços caso a vigência do contrato seja igual ou inferior a 12 (doze) meses e não tenha sido prorrogada, ou se ao tempo do término da contratação decorrerem 12 (doze) meses ou menos dos efeitos financeiros do último reajuste.

CLÁUSULA NONA – OBRIGAÇÕES DA CONTRATANTE

9.1. Exigir o cumprimento de todas as obrigações assumidas pela contratada, de acordo com o contrato e seus anexos;

9.2. Receber o objeto no prazo e condições estabelecidas no Termo de Referência;

9.3. Notificar a contratada, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele substituído, reparado ou corrigido, no total ou em parte, às suas expensas;

9.4. Nomear o fiscal e gestor do contrato por meio de Portaria a ser publicada no Diário da Assembleia.

9.5. Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pela contratada.

9.6. Comunicar a empresa para emissão de Nota Fiscal em relação à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.

9.7. Efetuar o pagamento à contratada do valor correspondente à execução do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência.

9.8. Aplicar à contratada as sanções previstas na lei e neste Contrato.

9.9. Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

9.10. Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pela contratada no prazo máximo de 1 (um) mês, admitida a prorrogação motivada por igual período.

9.11. A Administração não responderá por quaisquer compromissos assumidos pela contratada com terceiros, ainda que vinculados à execução do contrato, bem como por qualquer dano causado a terceiros em decorrência de ato da contratada, de seus empregados, prepostos ou subordinados.

CLÁUSULA DEZ – OBRIGAÇÕES DA CONTRATADA

10.1. Cumprir todas as obrigações constantes deste contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto.

10.2. Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior e prestar todo esclarecimento ou informação por eles solicitados.

10.3. Alocar os empregados necessários ao perfeito cumprimento das cláusulas deste contrato, com habilitação e conhecimento adequados, fornecendo os materiais, equipamentos, ferramentas e utensílios demandados, cuja quantidade, qualidade e tecnologia deverão atender às recomendações de boa técnica e a legislação de regência.

10.4. Reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no total ou em parte, no prazo fixado pelo fiscal do contrato, os serviços nos quais se verificarem vícios, defeitos ou incorreções resultantes da execução ou dos materiais empregados.

10.5. Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, de acordo com o Código de Defesa do Consumidor (Lei nº 8.078, de 1990), bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida no edital, o valor correspondente aos danos sofridos.

10.6. Não contratar, durante a vigência do contrato, cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, de dirigente do contratante ou do fiscal ou gestor do contrato, nos termos do artigo 48, parágrafo único, da Lei nº 14.133, de 2021.

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

10.8. Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local dos serviços.

10.9. Prestar todo esclarecimento ou informação solicitada pelo contratante ou por seus prepostos, garantindo-lhes o acesso, a qualquer tempo, ao local dos trabalhos, bem como aos documentos relativos à execução do empreendimento.

10.10. Paralisar, por determinação do contratante, qualquer atividade que não esteja sendo executada de acordo com a boa técnica ou que ponha em risco a segurança de pessoas ou bens de terceiros.

10.11. Promover a guarda, manutenção e vigilância de materiais, ferramentas, e tudo o que for necessário à execução do objeto, durante a vigência do contrato.

10.12. Conduzir os trabalhos com estrita observância às normas da legislação pertinente, cumprindo as determinações dos Poderes Públicos, mantendo sempre limpo o local dos serviços e nas melhores condições de segurança, higiene e disciplina.

10.13. Submeter previamente, por escrito, ao contratante, para análise e aprovação, quaisquer mudanças nos métodos executivos que fujam às especificações do memorial descritivo ou instrumento congênere.

10.14. Não permitir a utilização de qualquer trabalho do menor de dezesseis anos, exceto na condição de aprendiz para os maiores de quatorze anos, nem permitir a utilização do trabalho do menor de dezoito anos em trabalho noturno, perigoso ou insalubre.

10.15. Manter durante toda a vigência do contrato, em compatibilidade com as obrigações assumidas, todas as condições exigidas para habilitação na licitação.

10.16. Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação.

10.17. Guardar sigilo sobre todas as informações obtidas em decorrência do cumprimento do contrato.

10.18. Arcar com o ônus decorrente de eventual equívoco no dimensionamento dos quantitativos de sua proposta, inclusive quanto aos custos variáveis decorrentes de fatores futuros e incertos, devendo complementá-los, caso o previsto inicialmente em sua proposta não seja satisfatório para o atendimento do objeto da contratação, exceto quando ocorrer algum dos eventos arrolados no art. 124, II, d, da Lei nº 14.133, de 2021.

10.19. Cumprir, além dos postulados legais vigentes de âmbito federal, estadual ou municipal, as normas de segurança do contratante.

10.20. Verificar o recebimento de comunicações no endereço de e-mail indicado neste contrato a cada 24 (vinte e quatro) horas e informar ao contratante caso haja alteração de e-mail ou defeito técnico que impossibilite sua verificação, declarando estar ciente de que os prazos indicados nas comunicações se iniciam em 2 (dois) dias úteis a contar da data de envio do e-mail, salvo se houver confirmação de leitura ou de recebimento anterior, hipótese em que os prazos se iniciam com a respectiva confirmação.

CLÁUSULA ONZE – OBRIGAÇÕES PERTINENTES À LGPD

11.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.

11.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.

11.3. É vedado às partes a utilização de todo e qualquer dado pessoal repassado em decorrência da execução contratual para finalidade distinta daquela do objeto da contratação, sob pena de responsabilização administrativa, civil e criminal.

11.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pela contratada.

11.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever da contratada eliminá-los, com exceção das hipóteses do art. 16 da LGPD, incluindo aquelas em que houver necessidade de guarda de documentação para fins de comprovação do cumprimento de obrigações legais ou contratuais e somente enquanto não prescritas essas obrigações.

11.6. É dever da contratada orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.

11.7. A contratada deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.

11.8. O contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo a contratada atender prontamente eventuais pedidos de comprovação formulados.

11.9. A contratada deverá prestar, no prazo fixado pelo contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.

11.10. Bancos de dados formados a partir de contratos administrativos, notadamente aqueles que se proponham a armazenar dados pessoais, devem ser mantidos em ambiente virtual controlado, com registro individual rastreável de tratamentos realizados (LGPD, art. 37), com cada acesso, data, horário e registro da finalidade, para efeito de responsabilização, em caso de eventuais omissões, desvios ou abusos.

11.10.1. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.

11.11. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA DOZE – GARANTIA DE EXECUÇÃO

12.1. Não haverá exigência de garantia contratual da execução.

12.2. A garantia de execução é independente de eventual garantia do produto ou serviço prevista especificamente no Termo de Referência.

CLÁUSULA TREZE – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

13.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, a contratada que:

a) der causa à inexecução parcial do contrato;

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

c) der causa à inexecução total do contrato;

d) ensejar o retardamento da execução ou da entrega do objeto da licitação sem motivo

justificado;

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

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

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

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

13.2. Serão aplicadas à contratada que incorrer nas infrações acima descritas as seguintes sanções:

a) advertência, quando a contratada der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave;

b) impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c”, e “d” do subitem anterior, sempre que não se justificar a imposição de penalidade mais grave;

c) declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem anterior, bem como nas alíneas “b”, “c” e “d” que justifiquem a imposição de penalidade mais grave;

d) Multa, conforme tabela a seguir:

Tipo	Correspondência	Evento
Moratória	0,5% (meio por cento) do valor total mensal do contrato, por dia de atraso	Não atendimento a qualquer prazo estabelecido, pelo descumprimento ou inobservância a qualquer item estabelecido em prazo para execução e implantação;
Compensatória	1% (um por cento) do valor total do contrato, por ocorrência	Descumprimento ou inobservância a qualquer item estabelecido em Especificações Técnicas.
Compensatória	5% (cinco por cento) do valor total do contrato.	Infração descrita na alínea “a” do subitem anterior
Compensatória	10% (dez por cento) do valor total do contrato.	Infração descrita na alínea “b” do subitem anterior
Compensatória	20% (vinte por cento) do valor total do contrato.	Infração descrita na alínea “c” do subitem anterior
Compensatória	5% (cinco por cento) do valor do contrato.	Infração descrita na alínea “d” do subitem anterior
Compensatória	20% (vinte por cento) do valor total do contrato ou do valor estimado da contratação, quando for o caso.	Infrações descritas nos itens “e” a “f” do subitem anterior.
Compensatória	5% (cinco por cento) do valor total mensal do contrato.	Por indicador ou meta de nível de serviço, que tenha sido objeto de tentativa de burla, fraude, manipulação ou descaracterização pela Contratada.
Compensatória	2% (dois por cento) do valor total mensal do contrato	Por ocorrência que permaneça sem solução por mais de um período de faturamento consecutivo.

13.3. O atraso superior a 30 (trinta) dias autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

13.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao contratante.

13.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa.

13.6. A multa pode ser descontada da garantia, dos pagamentos devidos à Contratada em razão do contrato em que houve a aplicação da multa ou de eventual outro contrato havido entre a Alesc e a Contratada.

13.7. Além das disposições previstas na Lei nº 14.133/2021, o processo de aplicação de sanções contratuais seguirá o disposto no Ato da Mesa nº 257/2024.

13.8. Para os efeitos de aplicação das sanções acima descritas, considera-se como valor total do contrato o valor total da autorização de fornecimento ou documento equivalente.

13.9. A Meta de Atendimento e suporte será conforme tabela a seguir:

Atividade	**Nível Mínimo Serviço**	**Indicador Meta**	**Indicador**
Gerenciamento de regras	120 minutos após abertura do chamado	120 minutos	Regra implementada
Alteração de configurações	240 minutos após abertura do chamado	240 minutos	Configuração implementada
Verificação de Logs	24 horas após abertura do chamado	24 horas	Arquivo de log enviado ao solicitante
Atualização de plataformas, implantação de patches	5 dias após a liberação das atualizações pelo fabricante	5 dias	Patch e fix instalados
Registro de incidentes de segurança pela contratada	15 minutos após o primeiro registro ou sintoma relacionado ao evento	15 minutos	Chamado aberto
Início de atuação para resolução de incidentes de segurança	15 minutos após abertura de chamado pelo cliente ou pela contratada	15 minutos	Registro das ações tomadas no chamado pelo responsável pela resolução
Resolução de incidentes que provoquem indisponibilidade	120 minutos	120 minutos	Chamado concluído
Alteração de política de segurança	120 minutos após a abertura do chamado	120 minutos	Política implantada

Resolução de incidentes que não provoquem indisponibilidade	240 minutos	240 minutos	Chamado concluído
Atendimento de chamados para esclarecimento de dúvidas	24 horas após abertura do chamado pelo cliente	24 horas	Chamado concluído
Realização periódica de scan de vulnerabilidades	Mensal	30 dias	Relatórios de vulnerabilidades apresentados
Realização de implantação de patches de segurança de em ativos da rede	Mensal	30 dias	Relatórios de resultado da implantação
Realização de scan sob demanda	24 horas após a abertura do chamado	24 horas	Relatórios de vulnerabilidades apresentados

CLÁUSULA QUATORZE – DA EXTINÇÃO CONTRATUAL

14.1. O contrato será extinto quando vencido o prazo nele estipulado, independentemente de terem sido cumpridas ou não as obrigações de ambas as partes contraentes.

14.2. O contrato poderá ser extinto antes do prazo nele fixado, sem ônus para o contratante, quando esta não dispuser de créditos orçamentários para sua continuidade ou quando entender que o contrato não mais lhe oferece vantagem.

CLÁUSULA QUINZE – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas pertinentes ao objeto do presente Contrato correrão à conta da Fonte 1.5.00.100000, Subação 001369 (Manutenção, Serviços e Equipamento de Informática), Naturezas de Despesa 33.90.40.11 - Locação de Softwares e 33.90.40.08 - Manutenção de Softwares do Orçamento da Alesc.

CLÁUSULA DEZESSEIS – DOS CASOS OMISSOS

16.1. Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei nº 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei nº 10.406, de 2002 – Código Civil Brasileiro –, na Lei nº 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DEZESSETE – ALTERAÇÕES

17.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos artigos 124 e seguintes da Lei nº 14.133, de 2021.

17.2. A contratada é obrigada a aceitar, nas mesmas condições contratuais, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor inicial atualizado do contrato.

17.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da Procuradoria Jurídica do contratante, salvo nos casos de justificada necessidade de antecipação de seus efeitos, hipótese em que a formalização do aditivo deverá ocorrer no prazo máximo de 1 (um) mês.

17.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de

2021.

CLÁUSULA DEZOITO – DA LEI ANTICORRUPÇÃO

18.1. As partes comprometem-se a observar os preceitos legais instituídos pelo ordenamento jurídico brasileiro no que tange ao combate à corrupção, em especial, nas Leis nº 8.429/1992 e nº 12.846/2013, seus regulamentos e eventuais outras aplicáveis.

18.2. A contratada declara, por si e por seus administradores, funcionários, representantes e outras pessoas que agem em seu nome, direta ou indiretamente, estar ciente dos dispositivos contidos na Lei nº 12.846/2013; e se obriga a tomar todas as providências para fazer com que seus administradores, funcionários e representantes tomem ciência quanto ao teor da mencionada Lei nº 12.846/2013.

18.3. A contratada, no desempenho das atividades objeto deste contrato, compromete-se perante a contratante a abster-se de praticar ato(s) que possa(m) constituir violação à legislação aplicável ao presente instrumento pactual, incluindo aqueles descritos na Lei nº 12.846/2013, em especial no seu artigo 5º.

18.4. Qualquer descumprimento das regras da Lei Anticorrupção e suas regulamentações, por parte da contratada, em qualquer um dos seus aspectos, poderá ensejar a instauração do Procedimento de Apuração da Responsabilidade Administrativa – PAR, nos termos da legislação vigente, com aplicação das sanções administrativas porventura cabíveis e o ajuizamento de ação com vistas à responsabilização na esfera judicial, nos termos dos artigos 18 e 19 da Lei nº 12.846/2013.

18.5. A contratada declara que tem ciência de que a violação de qualquer das obrigações previstas neste contrato, além de outras, é causa para rescisão unilateral do contrato, sem prejuízo da cobrança das perdas e danos, inclusive danos potenciais, causados à parte inocente e das multas pactuadas.

18.6. A contratada compromete-se em notificar à Assembleia Legislativa do Estado de Santa Catarina qualquer irregularidade de que tiver conhecimento acerca da execução do presente contrato.

CLÁUSULA DEZENOVE – PUBLICAÇÃO

19.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021.

CLÁUSULA VINTE – FORO

20.1. Fica eleito o Foro da Comarca da Capital/SC para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

Florianópolis, documento datado e assinado digitalmente.

CONTRATANTE
Assembleia Legislativa do Estado de Santa Catarina (Alesc)

Leonardo Lorenzetti
Diretor-Geral

Brian Venceslau Michalski
Diretor de Tecnologia e Informações

CONTRATADA
[Representante Legal]

Documento assinado eletronicamente por **CARLOS ALBERTO LEAL**, **Coordenador de Licitações e Contratos**, em 30/05/2025, às 14:44, conforme art. 1º, III, "b", da Lei 11.419/2006.

Documento assinado eletronicamente por **LEONARDO LORENZETTI**, **Diretor-Geral**, em 02/06/2025, às 11:09, conforme art. 1º, III, "b", da Lei 11.419/2006.

A autenticidade do documento pode ser conferida no site https://sei.alesc.sc.gov.br/verifica-assinatura informando o código verificador **1740544** e o código CRC **287A7AA8**.