



EDITAL

PREGÃO ELETRÔNICO Nº 024/2024

(Processo SEI Nº 23.0.000030861-7)

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**, tipo **MENOR PREÇO**, mediante as condições estabelecidas neste Edital e em seus Anexos.

DATA DA SESSÃO PÚBLICA DO PREGÃO ELETRÔNICO

DIA: 18/06/2024

ABERTURA DA SESSÃO: 14:00

ENDEREÇO ELETRÔNICO: www.compras.gov.br

UASG: 929488

TIPO: menor preço por lote único

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 e nº 195, de 16 de junho de 2020;
- Autorização para Processo Licitatório – Despacho SEI Nº 1067377; e
- Processo SEI Nº 23.0.000030861-7.

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	Declaração de cumprimento da Lei nº 13.709/2018
Anexo	V	Modelo de Declaração de que atende às Leis estaduais nº 10.732/98 e nº 16.003/13
Anexo	VI	Minuta do Contrato

DO OBJETO

1. A presente licitação tem como objeto a contratação de ferramenta para gerenciamento de vulnerabilidades em servidores, estações de trabalho e ativos de rede, incluindo instalação, configuração, suporte garantia e treinamento, em conformidade com as especificações constantes neste Edital e seus Anexos.
2. A licitação será feita em lote único, 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\$ 896.791,77 (oitocentos e noventa e seis mil, setecentos e noventa e um reais e setenta e sete centavos), conforme Planilha de Valores Máximos Admissíveis.
5. As despesas pertinentes ao objeto do presente Edital correrão à conta da Subação 001369 (Manutenção, serviços e equipamentos de informática), Fonte do Recurso 1.500.100.000 (Recursos Não Vinculados de Impostos - Receita Líquida Disponível - RLD - Fonte Tesouro - EC), Natureza da Despesa 33.90.40.11 (Locação de Softwares); 33.90.40.08 (Manutenção de Softwares); e 33.90.39.48 (Serviços de Seleção e Treinamento) 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**, 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 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. 1º 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 7º, XXXIII, da Constituição;
- f) não ultrapassou o limite de faturamento e cumpre os requisitos estabelecidos do art. 3º da Lei Complementar nº 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 nº 8.213, de 24 de julho de 1991, esta 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. 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.

18. 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.

19. 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.

20. 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.

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

22. Qualquer elemento que possa identificar o licitante importará desclassificação da proposta, sem prejuízo das sanções previstas neste edital.

ABERTURA DA SESSÃO PÚBLICA

23. 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.

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

25. 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

26. 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.

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

DA FORMULAÇÃO DE LANCES

28. 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.

29. 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 (conforme consta no Anexo dos Valores Máximos Admissíveis), que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta.

30. 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.

31. 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.

32. 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.

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

34. 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.

35. 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.

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

37. 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.

38. 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

39. 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.

DA NEGOCIAÇÃO

40. 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.

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

DA ACEITABILIDADE DA PROPOSTA

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

43. 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 para o e-mail licitacoes@alesc.sc.gov.br, em até 2 (duas) horas, contadas da solicitação do Pregoeiro no sistema.

44. O Pregoeiro examinará a proposta mais bem classificada quanto à compatibilidade do preço ofertado com o valor máximo estipulado para o lote único, 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.

45. 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.

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

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

48. 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.

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

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

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

52. 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.

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

54. 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.

55. 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

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

57. 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.

58. 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.

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

60. Os licitantes deverão encaminhar no prazo estipulado pelo Pregoeiro, via sistema eletrônico, a seguinte documentação complementar:

- a) declaração de cumprimento da Lei Geral de Proteção de Dados - Lei n. 13.709/2018, devendo utilizar o modelo anexo a este edital;
- b) declaração de que atende as leis estaduais nº 10.732/98 e nº 16.003/2013, devendo utilizar o modelo anexo a este edital;
- c) apresentação de, no mínimo, 01 (um) atestado de capacidade técnico operacional, em nome da licitante, expedido por uma pessoa jurídica de direito público ou privado, comprovando a experiência no fornecimento prestação de serviços de implementação de ambientes utilizando este produto, dentro do território nacional.

d) fica dispensada de apresentação de atestado de capacidade técnica a licitante que subcontratar o fabricante da solução para a execução dos serviços exigidos no presente Edital. Neste caso a licitante deverá apresentar declaração do fabricante para comprovação do presente item.

e) a licitante deverá ser certificada como distribuidor oficial da marca oferecida, comprovando através de carta do fabricante especificamente para este edital.

61. Quando não constante no SICAF, o licitante deverá apresentar a seguinte documentação para fins de habilitação:

- a) prova de regularidade perante a Fazenda Federal;
- b) prova de regularidade perante a Fazenda Estadual;
- c) 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;
- d) prova de regularidade perante a Fazenda Municipal do domicílio ou sede do licitante;
- e) prova de regularidade com o FGTS;
- f) prova de regularidade com a Justiça do Trabalho;
- g) certidão negativa de efeitos de falência, recuperação judicial ou recuperação extrajudicial expedida pelo distribuidor da sede do licitante.

62. 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.

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

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

65. 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.

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

67. 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.

68. 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.

69. 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.

70. 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.

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

72. 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

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

74. 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.

75. 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.

76. 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.

77. A apreciação se dará em fase única.

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

DA ADJUDICAÇÃO E HOMOLOGAÇÃO

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

80. 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

81. Depois de homologado o resultado deste Pregão, o licitante vencedor será convocado para assinatura do contrato, e terá o prazo de até 5 (cinco) dias úteis para efetuar sua assinatura, sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital e na Lei nº 14.133/2021.

a) 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.

82. O licitante deverá manter atualizado o seu endereço *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.

83. 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.

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

85. Os encargos das partes, suas obrigações e as normas relativas a pagamento constam do Termo de Referência e/ou minuta do contrato encartado neste Edital.

86. 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

87. As sanções administrativas às quais o licitante estará sujeito estão previstas nos Termo de Referência e minuta do contrato, encartados neste Edital.

DOS ESCLARECIMENTOS E DA IMPUGNAÇÃO AO EDITAL

88. 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.

89. A Coordenadoria de Licitações e Contratos, auxiliada pelo setor técnico ou comissão competente, decidirá sobre a impugnação do certame.

90. 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.

91. Os pedidos de esclarecimentos devem ser enviados à Coordenadoria de Licitações e Contratos até 03 (três) dias úteis antes da data fixada para abertura da sessão pública, exclusivamente para o endereço eletrônico licitacoes@alesc.sc.gov.br.

92. 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

93. 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 nº 14.133/2021.

94. 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.

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

96. 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.

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

98. Este pregão poderá ter a data de abertura da sessão pública transferida por conveniência da ALESC

99. 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.

100. 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.

101. Integra o presente edital a minuta do contrato.

102. 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

103. 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.

Alexandre Lencina Fagundes
Diretor Geral

ANEXO I

EDITAL DE PREGÃO ELETRÔNICO Nº 024/2024

TERMO DE REFERÊNCIA

Aquisição de ferramenta para Gestão de Vulnerabilidades

1. Unidade Requisitante

Diretoria de Tecnologia de Informações - Coordenadoria de Redes.

2. Objeto

O presente objeto visa a contratação de uma ferramenta para gerenciamento de vulnerabilidades em servidores, estações de trabalho e ativos de rede, bem como o serviço de instalação, configuração, suporte garantia e treinamento.

3. Justificativa

A aquisição de uma ferramenta para gestão de vulnerabilidades é fundamental para garantir a segurança, integridade, confidencialidade e disponibilidade dos dados armazenados em servidores hospedados no datacenter da Assembleia Legislativa do Estado de Santa Catarina (ALESC) de forma que a ferramenta fará parte essencial do conjunto de medidas tomadas para que a entidade pública mantenha a conformidade com a Lei Geral de Proteção de Dados (LGPD). A implementação de tal ferramenta permitirá identificar e remediar potenciais brechas de segurança de forma proativa, minimizando o risco de violações de dados, vazamentos de informações sensíveis e comprometimento da imagem da instituição decorrentes de incidentes cibernéticos. Além disso, a gestão de vulnerabilidades proporciona a manutenção de um ambiente tecnológico robusto, assegurando a continuidade dos serviços e a proteção das informações sensíveis dos clientes e servidores da ALESC, fortalecendo a reputação da entidade pública e demonstrando o compromisso com a segurança da informação.

3.1 Prova de conceito

Durante a elaboração do presente documento, foram realizadas provas de conceito (PoC) com alguns provedores de soluções de gerenciamento de vulnerabilidades, à exemplo: Qualys Security, Tenable e Ridge Security. Com a realização da PoC foi possível identificar diversos hosts, websites e aplicações com vulnerabilidades exploráveis, sendo objeto fundamental para entendimento do funcionamento das ferramentas. Também com o intuito de corroborar com as

afirmativas citadas, abaixo são apresentadas evidências de vulnerabilidades identificadas que tem potencial danoso para a ALESC, onde tais vulnerabilidades foram descobertas durante a PoC realizada com as empresas citadas.

4. Especificação

4.1 Da solução de gestão de vulnerabilidades

4.1.1 A solução deve ser entregue como um serviço Software-as-a-Service (SaaS) em uma nuvem proprietária do fabricante para todos os seus serviços e aplicativos exigidos neste documento. Serviços fornecidos por nuvens de terceiros não são aceitos.

4.1.2 A gestão de todos os módulos considerados neste termo deve ser feita através de uma console única

4.1.3 A solução deverá possuir no mínimo, duas das seguintes certificações de privacidade e segurança:

- i. EU-U.S. Privacy Shield Framework.
- ii. Swiss-U.S. Privacy Shield Framework.
- iii. Cloud Security Alliance
- iv. (CSA) STAR

4.1.4 Todos os serviços da plataforma devem estar disponíveis sob o mesmo padrão de qualidade de serviço 24x7x365 e garantir 99% de disponibilidade.

4.1.5 O ofertante deve oferecer manutenção e atualização constante da plataforma durante todo o período de vigência do contrato de serviço.

4.1.6 As atualizações de serviço devem ser transparentes para o administrador da solução, sem afetar nenhum dos dados armazenados - serviços fornecidos.

4.1.7 Todas as comunicações entre componentes, transferência de dados e sincronização da solução devem ser criptografadas de ponta a ponta, fazendo uso de no mínimo TLS 1.2, certificados assinados com RSA 2048 bits e algoritmo de assinatura SHA256.

4.1.8 A solução deve permitir criação de usuários distintos

4.1.9 Deve permitir separação de funções e permissões na console

4.1.10 Deve permitir integração através de SSO com, pelo menos, Azure Active Directory.

4.1.11 A console deve ser acessível a partir de, pelo menos, um dos navegadores comerciais dentre Google Chrome, Microsoft Edge e Firefox.

4.2 Dos agentes

4.2.1 A solução proposta deve oferecer um agente de baixo impacto nos sistemas operacionais onde está instalado e no consumo de largura de banda que utilizará na rede.

4.2.2 A solução deve ser instalada em servidores, estações de trabalho, e máquinas virtuais, suportando sua implantação em rede local, em rede doméstica e na nuvem.

4.2.3 A solução deve oferecer suporte para sua implantação em pelo menos os seguintes sistemas operacionais:

4.2.3.1 Windows 7/Windows Server 2003 SP2 e posterior (x86, x64)

4.2.3.2 Red Hat Enterprise Linux/CentOS 6.5+, 7.x (x64), 8.x (x64), 9.x (x64)

4.2.3.3 Debian 9 (x64), 10 (x64), 11 (x64) , 12 (x64)

4.2.3.4 Rocky Linux 8 (x64), 9(x64)

4.2.3.5 Ubuntu 14, 16,18,19,20,21,22 (x64)

4.2.3.6 Oracle Enterprise Linux 9, Oracle Enterprise Linux 8, Oracle Enterprise Linux (OEL) 7 até 7.5, Oracle Enterprise Linux (OEL) 6

4.2.3.7 SUSE Linux Enterprise Server (SLES) 12, SUSE Linux Enterprise Server (SLES) 11

4.2.3.8 FreeBSD 13.0, 12.2

4.2.4 O agente da solução deve se atualizar automaticamente e gerir as suas atualizações automaticamente.

- 4.2.5 A solução deve suportar plataformas de nuvem AWS, GCP, Azure.
- 4.2.6 A solução deve ser capaz de coletar informações sobre o inventário de ativos.
- 4.2.7 As funcionalidades de gestão de ativos, gestão de vulnerabilidade e detecção de patches devem ser fornecidas pelo mesmo agente de gerenciamento, não serão aceitas soluções com múltiplos agentes.
- 4.2.8 A solução deve prover nativamente um dispositivo capaz de concentrar requisições dos agentes para encaminhamento a console de gerenciamento de forma a evitar a conexão direta de agentes com a plataforma
- 4.2.9 O agente de gerenciamento deve suportar o uso de proxy
- 4.2.10 Deve ser possível definir o intervalo de comunicação entre o agente e a console de gerenciamento
- 4.2.11 Deve ser possível limitar o consumo de CPU e memória do agente
- 4.2.12 Deve permitir a definição de um período global de inatividade dos agentes

4.3 Dos scanners

- 4.3.1 A solução deve permitir o uso de scanners capazes de identificar vulnerabilidades através de varreduras em ranges de IP definidos pelo administrador
- 4.3.2 Não deverá haver restrições para instalação de scanners virtuais no ambiente.
- 4.3.3 Deve ser permitido o uso de scanners externos, sem necessidade de instalação, em nuvem própria do fabricante para varreduras de ativos publicados na internet.
- 4.3.4 Os scanners virtuais devem suportar pelo menos um dos hypervisors abaixo:
 - 4.3.4.1 VMWare
 - 4.3.4.2 Hyper-V
 - 4.3.4.3 OpenShift / KVM
- 4.3.5 Os Scanners devem suportar a varredura de ambientes em nuvem para pelo menos os seguintes provedores:
 - 4.3.5.1 Azure
 - 4.3.5.2 AWS
 - 4.3.5.3 Google Cloud Platform
 - 4.3.5.4 Oracle
- 4.3.6 Os scanners devem reportar vulnerabilidades para console em nuvem, permitindo uma visão consolidada de vulnerabilidades
- 4.3.7 Deve ser permitido o agendamento de varreduras para máquinas que possuam uma determinada versão de banco de dados em execução
- 4.3.8 Deve ser permitido a varredura sob demanda para um ou mais ativos de rede
- 4.3.9 O mesmo scanner deve ser capaz de varrer por falhas de conformidade e por vulnerabilidades
- 4.3.10 O scanner deverá consolidar vulnerabilidades encontradas em um ativo que possua agente instalado.
- 4.3.11 A solução deve permitir a configuração do tipo de varredura a ser realizada, permitindo pelo menos definir as seguintes configurações ao defini-la:
 - 4.3.11.1 Configuração de quantidades de portas TCP/UDP a serem validadas
 - 4.3.11.2 Consumo de largura de banda e recursos (alto, médio, baixo)
 - 4.3.11.3 Digitalize para dispositivos que não suportam Ping - traceroute
 - 4.3.11.4 Detecção de balanceadores de carga
 - 4.3.11.5 Configuração de força bruta para usar em senhas
 - 4.3.11.6 Uso de um cabeçalho HTTP personalizado
 - 4.3.11.7 Ignorar pacotes
 - 4.3.11.8 Instalação de agente temporário para validação de registro local

4.4 Da categorização e inventário dos ativos

- 4.4.1 A solução proposta deve permitir a coleta de informações detalhadas sobre o ativo gerenciado, deve detalhar pelo menos os seguintes dados para cada ativo:

- 4.4.1.1 Serviços em execução
- 4.4.1.2 Software instalado
- 4.4.1.3 Usuários
- 4.4.1.4 Portas abertas
- 4.4.1.5 Nome do host
- 4.4.1.6 FQDN
- 4.4.1.7 IP v4 / v6
- 4.4.1.8 Endereço MAC
- 4.4.1.9 Processador
- 4.4.1.10 Memória
- 4.4.1.11 Volumes de disco
- 4.4.1.12 BIOS
- 4.4.2 A solução deve classificar automaticamente os ativos por famílias de tecnologia, tipo de dispositivo, tipo de plataforma e fabricante.
- 4.4.3 A solução deve normalizar automaticamente os nomes dos fabricantes de HW e SW com seus dados relevantes, como o nome dos aplicativos e versões, para facilitar sua posterior busca na solução.
- 4.4.4 A solução deve possuir a habilidade de etiquetagem (Tags) de ativos para facilitar a identificação, deve permitir a geração de Tags, pelo menos, usando os seguintes parâmetros:
 - 4.4.4.1 Palavras-chave
 - 4.4.4.2 Endereço IP e intervalos de IP
 - 4.4.4.3 Segmento de rede
 - 4.4.4.4 Portas abertas
 - 4.4.4.5 Informações de inventário considerando, no mínimo:
 - 4.4.4.5.1 Sistema operacional,
 - 4.4.4.5.2 Presença ou ausência de determinado software instalado ou serviço em execução
 - 4.4.4.6 Última localização geográfica detectada incluindo cidade e país
 - 4.4.4.7 Groovy Scriptlet
 - 4.4.4.8 Regex
- 4.4.5 A solução deve permitir agrupamento manual a critério do administrador da solução.
- 4.4.6 A solução deve permitir atribuir criticidade ao ativo para priorizá-lo durante o processo de gerenciamento.
- 4.4.7 Deve permitir criação de Dashboards personalizados que sejam capazes de trazer as seguintes informações sobre os ativos:
 - 4.4.7.1 Categorias de softwares instalados nos ativos
 - 4.4.7.2 Hosts que executam máquinas virtuais
 - 4.4.7.3 Sistemas operacionais utilizados
 - 4.4.7.4 Serviços e portas TCP ou UDP abertas
 - 4.4.7.5 Softwares de segurança instalados
 - 4.4.7.6 Memória total utilizada
 - 4.4.7.7 Quantidade de processadores
 - 4.4.7.8 Quantidade de armazenamento disponível
- 4.4.8 A solução deve permitir uma interface de busca de ativos que utilize uma sintaxe lógica baseados, no mínimo, nos critérios abaixo:
 - 4.4.8.1 Fabricante de hardware
 - 4.4.8.2 Último usuário logado
 - 4.4.8.3 Categoria de software instalado
- 4.4.9 A solução deve permitir a visualização de quantidade de máquinas com um determinado software instalado
- 4.4.10 Deve permitir visualização de recursos em nuvem AWS ou Azure tais como VPCs,

Virtual Networks, Security Group, s3 buckets, RDS, SQL Server, sem necessidade de instalação de agentes ou varreduras de rede.

4.4.11 Deve permitir visibilidade a respeito de hosts que executam containers e containers em execução

4.5 Da gestão de vulnerabilidades, detecção e resposta

4.5.1 A solução deve permitir **descobrir, avaliar, priorizar** e auxiliar na **correção de vulnerabilidades / configurações** em toda a infraestrutura de rede, incluindo estações de trabalho, servidores, dispositivos de rede, dispositivos de telecomunicações e dispositivos de segurança, hypervisors, máquinas virtuais, orquestradores de contêineres, contêineres e nuvens (Azure, GCP, AWS), proporcionando através de única interface para o administrador via um portal web para gerenciamento de todos os ativos, permitindo o gerenciamento centralizado de todos os componentes da solução a partir de um único ponto, sem a necessidade de incorrer em consoles - componentes adicionais fora dele para a administração dos serviços oferecidos.

4.5.2 A solução deve ser oferecida na modalidade SaaS em nuvem própria do fabricante, sem necessidade de instalação de componentes locais para a gerência.

4.5.3 A solução deve ser licenciada por Asset (IP - HOST) para ativos de infraestrutura

4.5.4 A solução deve ser licenciada por URLs para varreduras de aplicação web.

4.5.5 A solução deve ser licenciada para **300 IP / HOST para varredura de vulnerabilidade, 300 HOST para Patch / Inventário, 100 URLs para varredura e scans de aplicações web.**

4.5.6 Gestão de Vulnerabilidade

4.5.6.1 A solução deve permitir varreduras de vulnerabilidade com base em:

4.5.6.1.1 Sistemas Operacionais

4.5.6.1.2 Serviços WEB

4.5.6.1.3 Portas TCP e UDP

4.5.6.1.4 Serviços

4.5.6.1.5 Aplicações

4.5.6.1.6 Bancos de dados

4.5.6.1.7 Dispositivos de rede como switches, roteadores e balanceadores de carga

4.5.6.2 No mínimo, a ferramenta deve abranger os seguintes sistemas operacionais, bancos de dados e aplicativos.

4.5.6.2.1 Microsoft Windows

4.5.6.2.2 UNIX

4.5.6.2.3 LINUX

4.5.6.2.4 MacOS

4.5.6.2.5 Mac OS X

4.5.6.2.6 Cisco

4.5.6.2.7 VMware

4.5.6.3 Detectar e analisar vulnerabilidades nas principais versões de Bancos de Dados, pelo menos:

4.5.6.3.1 Microsoft SQL Server

4.5.6.3.2 MySQL

4.5.6.3.3 Oracle

4.5.6.3.4 Sybase

- 4.5.6.3.5 PostgreSQL**
- 4.5.6.3.6 Cache**
- 4.5.6.3.7 Db2**
- 4.5.6.4 Detectar e analisar vulnerabilidades em plataformas WEB, pelo menos:**
 - 4.5.6.4.1 IIS**
 - 4.5.6.4.2 Apache**
 - 4.5.6.4.3 Wordpress**
 - 4.5.6.4.4 Apache Tomcat**
 - 4.5.6.4.5 JBoss**
 - 4.5.6.4.6 NGINX**
 - 4.5.6.4.7 Drupal**
 - 4.5.6.4.8 Joomla!**
 - 4.5.6.4.9 Media Wiki**
- 4.5.6.5 Detectar e analisar vulnerabilidades em portas e serviços TCP e UDP**
- 4.5.6.6 Detectar vulnerabilidades em pelo menos os seguintes aplicativos ou plataformas:**
 - 4.5.6.6.1 Adobe (pdf, creative)**
 - 4.5.6.6.2 Apple**
 - 4.5.6.6.3 HP**
 - 4.5.6.6.4 Microsoft (Office, IIS, Exchange)**
 - 4.5.6.6.5 Oracle**
 - 4.5.6.6.6 Oracle Java**
 - 4.5.6.6.7 VMware**
 - 4.5.6.6.8 Cisco**
 - 4.5.6.6.9 Checkpoint**
- 4.5.6.7 Permitir a descoberta de vulnerabilidades na rede, oferecendo as seguintes alternativas de varredura:**
 - 4.5.6.7.1 Varredura ativa de rede não autenticada**
 - 4.5.6.7.2 Varredura ativa de rede autenticada**
 - 4.5.6.7.3 Agente**
 - 4.5.6.7.4 Varreduras externas**
- 4.5.6.8 O mecanismo de varredura deve ter uma taxa de precisão de detecção de vulnerabilidade de 99,99966% (seis sigma) durante os últimos 10 anos.**
- 4.5.6.9 A base de conhecimento de vulnerabilidade deve ser atualizada semanalmente, garantindo a incorporação de pelo menos 20 CVEs a ela e deve ter pelo menos uma base de conhecimento de 40.000 CVEs relacionados incluindo tecnologias legadas e atuais.**
- 4.5.6.10 A solução deve oferecer suporte ao padrão da indústria para pontuação de vulnerabilidade do Common Vulnerability Scoring System (CVSS)**
- 4.5.6.11 A solução deve oferecer suporte ao padrão da indústria para adicionar detecções personalizadas usando Open Vulnerability Assessment Language (OVAL).**
- 4.5.6.12 A solução deve permitir vincular as vulnerabilidades detectadas e indicar sua relação com ameaças como Vírus, Trojan e Malware.**
- 4.5.6.13 A solução deve ser capaz de indicar explorações disponíveis e códigos disponíveis para uma vulnerabilidade, quando aplicável**
- 4.5.6.14 O banco de dados deve relacionar a maioria das vulnerabilidades ao CVE e Bugtraq.**
- 4.5.6.15 A solução deve oferecer suporte à integração para autenticação por ferramentas de cofres de senha com ao menos duas dos seguintes fabricantes, Thycotic/Centrify, CyberArk, BeyondTrust**
- 4.5.6.16 A solução deve permitir buscas interativas de vulnerabilidade utilizando filtros como severidade, categoria, sistema operacional, status, classificação do CVSS, CVE ou KB.**

- 4.5.6.17** A solução deve permitir a utilização de operadores lógicos na busca de vulnerabilidades para que seja possível encontrar, no mínimo, as seguintes informações:
- 4.5.6.17.1** Vulnerabilidades associadas a ransomware e que possuem patches disponíveis
 - 4.5.6.17.2** Vulnerabilidades detectadas em um segmento de rede
 - 4.5.6.17.3** Vulnerabilidades detectadas em serviços específicos
 - 4.5.6.17.4** Vulnerabilidades detectadas por um usuário específico
 - 4.5.6.17.5** Vulnerabilidades detectadas por tag AWS ou Azure específicas
 - 4.5.6.17.6** Vulnerabilidades detectadas em hardware específico
- 4.5.6.18** Na busca de vulnerabilidades deve permitir agrupamento para mostrar, no mínimo, as seguintes visualizações:
- 4.5.6.18.1** Quantidade de ocorrências de uma mesma vulnerabilidade
 - 4.5.6.18.2** Quantidade de vulnerabilidades por sistema operacional
 - 4.5.6.18.3** Quantidade de vulnerabilidades por host
 - 4.5.6.18.4** Quantidade de vulnerabilidades por Exploit disponível
 - 4.5.6.18.5** Quantidade de vulnerabilidades por produto/software vulnerável
- 4.5.6.19** A solução deve permitir exportar buscas e filtros criados para um dashboard
- 4.5.6.20** A solução deve permitir salvar filtros criados em buscas para reutilização
- 4.5.6.21** Deve mostrar dashboards que consigam mostrar variação histórica de vulnerabilidades novas, corrigidas, reabertas
- 4.5.6.22** Deve permitir mostrar dashboards que contenham quantidades de vulnerabilidades associadas a ramsonware, que contém exploits públicos e que permitem exploração sem autenticação
- 4.5.6.23** **Deve mostrar dashboards que mostrem o racional de vulnerabilidades que podem ser corrigidas através de patches**
- 4.5.6.24** Deve mostrar patches faltantes em sistemas operacionais independente da relação com uma vulnerabilidade existente
- 4.5.6.25** A solução deve oferecer a possibilidade de monitorar dispositivos móveis Android, IOS, IpadOS

4.6 Da gestão de configuração

- 4.6.1** **A solução deve permitir a avaliação, o relatório e o relatório de problemas de configuração, com base nas referências do padrão da indústria do Centro de Segurança da Internet (CIS).**
- 4.6.2** O fabricante deve ser oficialmente certificado pelo CIS para fornecer este nível de controles.
- 4.6.3** A solução deve oferecer avaliação de configuração com base no benchmark CIS padrão da indústria, cobrindo esta funcionalidade nas seguintes categorias:
- 4.6.3.1** Sistemas operacionais
 - 4.6.3.2** Software de servidor
 - 4.6.3.3** Provedores de nuvem
 - 4.6.3.4** Dispositivos de rede
 - 4.6.3.5** Software de desktop
- 4.6.4** A solução deve suportar detecção de falhas de conformidades através de varreduras autenticadas ou através de agente instalado diretamente no ativo monitorado.
- 4.6.5** A solução deve permitir que os administradores recebam informação de conformidade de sistemas operacionais Windows e Linux, mesmo que não estejam conectados à rede corporativa.
- 4.6.6** A solução deve permitir a avaliação de certificados digitais (internos e externos) e configurações de TLS em busca de problemas e vulnerabilidades de certificados, resultando em diferentes graus de conformidade de acordo com os resultados da

avaliação de seu emissor, prazo de validade, tipo de certificado, robustez do o algoritmo e o conjunto de criptografia usados.

4.7 Da detecção e priorização de ameaças

- 4.7.1** A solução proposta deve permitir enviar alertas em tempo real sobre irregularidades na rede, identificar ameaças e monitorar mudanças inesperadas que ocorram na mesma.
- 4.7.2** A solução deve permitir enviar notificações para usuários específicos e grupos de usuários para o perfil de monitoramento - perfis de monitoramento múltiplos.
- 4.7.3** A solução deve permitir a personalização do perfil de monitoramento associado a uma lista específica de critérios.
- 4.7.4** A solução deve permitir que os alertas sejam personalizados para uma ampla variedade de condições que afetam sistemas, certificados, vulnerabilidades, portas, serviços e software. Cada regra deve permitir que seja configurada para detectar mudanças gerais comuns - para se ajustar a circunstâncias muito específicas.
- 4.7.5** A solução deve permitir a atribuição de destinatários diferentes para cada alerta.
- 4.7.6** A solução deve enviar alertas de monitoramento sobre vulnerabilidades, configurações incorretas e outros parâmetros definidos pelo administrador da solução, como:
 - 4.7.6.1** Ativos com sistemas operacionais não aprovados
 - 4.7.6.2** Certificados expirados - expirando
 - 4.7.6.3** Portas abertas
 - 4.7.6.4** Vulnerabilidades graves
 - 4.7.6.5** Tickets de correção abertos, resolvidos e fechados
 - 4.7.6.6** Software não aprovado
- 4.7.7** A solução proposta deve fornecer fontes de inteligência de ameaças em tempo real e técnicas de aprendizado de máquina para fornecer controle de administrador sobre a evolução das ameaças relacionadas a vulnerabilidades encontradas nos ativos da organização e identificar quais corrigir primeiro.
- 4.7.8** A solução deve permitir consultas Ad-Hoc com múltiplas variáveis e critérios, como classe de ativo, tipo de vulnerabilidade, indicadores de ameaça em tempo real, etiqueta de ativo e sistema operacional, de modo que, por exemplo, seja possível pesquisar todas as vulnerabilidades que tenham uma alta classificação de gravidade, são fáceis de explorar e foram lançados na semana passada.
- 4.7.9** A solução deve permitir que se faça uma correlação em tempo real das ameaças ativas contra as vulnerabilidades detectadas nos ativos corporativos.
- 4.7.10** A solução deve incluir indicadores de ameaças em tempo real que ajudam a avaliar e priorizar as vulnerabilidades detectadas, categorizados da seguinte forma:
 - 4.7.10.1** Dia Zero: vulnerabilidades para as quais não há patch disponível e para as quais um ataque ativo foi observado.
 - 4.7.10.2** Exploração pública: Vulnerabilidades cujo mecanismo de exploração é conhecido, para o qual existe um código de exploração e está disponível publicamente.
 - 4.7.10.3** Ataques ativos: vulnerabilidades que estão sendo atacadas ativamente.
 - 4.7.10.4** Movimento lateral: vulnerabilidades que permitem ao invasor espalhar o ataque amplamente pela rede violada.
 - 4.7.10.5** Fácil exploração: vulnerabilidades que podem ser facilmente exploradas, exigindo poucas habilidades e pouco conhecimento
 - 4.7.10.6** Perda de dados: vulnerabilidades cuja exploração causará perda massiva de dados
 - 4.7.10.7** Negação de serviço: vulnerabilidades cuja carga útil pode sobrecarregar - impedir que sistemas comprometidos estejam permanentemente - temporariamente disponíveis.
 - 4.7.10.8** No Patch: Vulnerabilidades para as quais não há solução do provedor
 - 4.7.10.9** Malware: vulnerabilidades associadas a infecções por malware
 - 4.7.10.10** Kit de exploração: vulnerabilidades para as quais um kit de exploração está

disponível

- 4.7.11 A solução deve atribuir uma pontuação a cada vulnerabilidade de forma contextual de forma a quantificar o risco associado a esta vulnerabilidade.
- 4.7.12 Os fatores de risco devem considerar, pelo menos 3 dos fatores abaixo:
 - 4.7.12.1 Malwares associados
 - 4.7.12.2 Atores maliciosos associados
 - 4.7.12.3 Possibilidade de remediação
- 4.7.13 A solução proposta deve fornecer um workflow de correção baseado em políticas de criação e atribuição, atribuindo tickets de acordo com as condições definidas pelo administrador da solução através de políticas ou manualmente.
- 4.7.14 A solução deve permitir a criação de tickets com status aberto, fechado, ignorado, com base nos seguintes critérios:
 - 4.7.14.1 Host(s) a quem a regra se aplica
 - 4.7.14.2 Vulnerabilidade (s) a que a regra se aplica
 - 4.7.14.3 Usuário atribuído
 - 4.7.14.4 Data de criação - expiração
 - 4.7.14.5 Mudança de estado
- 4.7.15 A solução deve permitir a criação de tickets de correção automaticamente a partir do resultado de uma varredura de vulnerabilidade - com base nas informações de um host específico e manualmente por um administrador de solução.

4.8 Do gerenciamento de patches

- 4.8.1 A solução proposta deve correlacionar vulnerabilidades e patches automaticamente para os hosts da sua organização.
- 4.8.2 A solução deve mapear automaticamente os patches com CVEs associados às vulnerabilidades detectadas.
- 4.8.3 Deve mostrar patches faltantes mesmo que não exista correlação com uma vulnerabilidade existente
- 4.8.4 Deve mostrar patches faltantes para no mínimo as seguintes categorias
 - 4.8.4.1 Navegadores
 - 4.8.4.2 Ferramentas de compressão de arquivos
 - 4.8.4.3 Visualizadores de PDF
 - 4.8.4.4 Editores de texto e planilhas
 - 4.8.4.5 Sistemas operacionais

4.9 Dos relatórios e dashboards

- 4.9.1 A solução proposta deve permitir administração centralizada via interface gráfica WEB usando HTTPS.
- 4.9.2 A solução deve possibilitar o acesso a console de todos os componentes do serviço a partir de um único ponto.
- 4.9.3 A solução deve permitir a definição de diferentes perfis de usuários e funções para administração.
- 4.9.4 A solução deve fornecer controles de acesso de usuário hierárquicos e baseados em funções que permitem a delegação de responsabilidades para refletir a estrutura organizacional.
- 4.9.5 A solução deve permitir o acesso de um usuário autorizado de qualquer local.
- 4.9.6 A solução deve suportar integração com uma biblioteca API XML extensível.
- 4.9.7 A solução deve suportar autenticação de dois fatores para usuários e login.
- 4.9.8 A solução deve suportar configurações de segurança de senha.
- 4.9.9 A solução deve suportar personalizar a política de segurança para configurações de gerenciamento de senha, por:
 - 4.9.9.1 Idade e expiração da senha.
 - 4.9.9.2 Conta do usuário bloqueada após uma série de logins com falha.

- 4.9.9.3 Comprimento mínimo da senha.
- 4.9.9.4 Complexidade da senha, caracteres alfanuméricos e numéricos a serem usados.
- 4.9.9.5 Forçar mudança de senha no login inicial
- 4.9.9.6 Notificação de senha expirada antes de vários dias.
- 4.9.10 A solução deve suportar a capacidade de restringir o acesso apenas de rede interna da instituição.
- 4.9.11 A solução deve suportar a capacidade de rastrear a atividade do usuário por nome da conta do usuário, data, ação e informações sobre a ação.
- 4.9.12 **A solução deve suportar a capacidade de distribuir relatórios em PDF com segurança por meio de uma senha e um número restrito de download de relatórios por meio do link.**
- 4.9.13 A solução deve suportar acesso por SSO (Single Sign-on) usando SAML 2.0.
- 4.9.14 A solução deve permitir o controle de alterações com trilhas de auditoria à prova de violação.
- 4.9.15 A solução proposta deve gerar relatórios por IPs, Grupo e Tags:
- 4.9.16 A solução deve permitir a geração de relatórios de qualquer IP - Host previamente verificado.
- 4.9.17 A solução deve permitir agendar relatórios diários, semanais, mensais e sob demanda.
- 4.9.18 A solução deve permitir o envio de notificações por email sempre que um relatório estiver disponível para o administrador da solução, usuários específicos e perfis diferentes criados na ferramenta.
- 4.9.19 A solução deve permitir pelo menos os seguintes tipos de relatórios:
 - 4.9.19.1 Relatório de correção
 - 4.9.19.2 Relatório de vulnerabilidades altamente críticas
 - 4.9.19.3 Relatório Executivo
 - 4.9.19.4 Relatório de autenticação
 - 4.9.19.5 Relatório de conformidade normativa e regulatória
 - 4.9.19.6 Relatório de remediação
- 4.9.20 A solução deve fornecer relatórios de correção por grupo de ativos, usuário e vulnerabilidade.
- 4.9.21 A solução deve permitir a criação de relatórios baseados em IPv4, endereços IPv6, nome do host, grupo de ativos e rótulos personalizados pelo administrador.
- 4.9.22 A solução deve permitir relatórios com cálculo de risco de segurança, permitindo um cálculo de risco global para todos os ativos incluídos no relatório.
- 4.9.23 A solução deve permitir relatórios que possibilitem o cálculo do risco do negócio, utilizando como base para o cálculo do risco de impacto ao negócio e do risco de segurança dos ativos incluídos no relatório.
- 4.9.24 A solução deve permitir relatar as descobertas com base no status das vulnerabilidades detectadas e seu status, conforme lista abaixo:
 - 4.9.24.1 Novo
 - 4.9.24.2 Resolvido
 - 4.9.24.3 Reaberto
 - 4.9.24.4 Ativo
- 4.9.25 A solução deve permitir relatórios que incluam vulnerabilidades com base na data de publicação.
- 4.9.26 A solução deve permitir incluir - excluir kernels Linux detectados na varredura de vulnerabilidade e que não estão em execução.
- 4.9.27 A solução deve permitir a exclusão de vulnerabilidades que você encontrará em uma porta ou serviço que não está em execução.
- 4.9.28 A solução deve permitir excluir vulnerabilidades que não são exploráveis devido à configuração do sistema / plataforma onde foi detectada.
- 4.9.29 A solução deve permitir a exclusão de patches da Microsoft que foram substituídos por

um novo patch ou um patch cumulativo do mesmo fabricante.

4.9.30 A solução deve fornecer relatórios automatizados de tendências e diferenciais.

4.9.31 A solução deve fornecer várias opções de distribuição de relatórios, incluindo PDF criptografado.

4.9.32 A solução deve dar suporte à personalização do modelo de relatório conforme necessário.

4.9.33 A solução deve permitir a exportação de relatórios para os formatos HTML, MHT, PDF, DOC, CSV e XML

4.9.34 A solução deve permitir que relatórios sejam apresentados em tabelas e gráficos com as ocorrências ocorridas, permitindo a customização detalhada de cada relatório.

4.9.35 A solução deve permitir em seus relatórios comparar o nível de conformidade entre políticas, tecnologias e ativos.

4.9.36 A solução deve possuir um painel (dashboard) que, por padrão, permite que você veja as tendências de vulnerabilidades por gravidade, plataforma, idade e status de remediação.

4.9.37 A solução deve permitir a customização dos painéis fazendo uso de qualquer um dos dados disponíveis associados aos ativos varridos para selecionar diferentes tipos de gráficos, tabelas e visualizações sobre a priorização de vulnerabilidades.

4.9.38 A solução deve fornecer painéis executivos personalizáveis com uma visão unificada de todos os componentes da solução.

4.9.39 Deve ser possível criar dashboards que mostrem a pontuação de risco global de ativos e sua variação ao longo do tempo.

4.10 Da verificação e scan de aplicações WEB

4.10.1 A solução proposta deve habilitar varreduras profundas dinâmicas para descobrir e catalogar todos os aplicativos da web e APIs na rede corporativa externa, redes corporativas internas e instâncias de nuvem.

4.10.2 A solução deve permitir varreduras autenticadas, complexas e progressivas.

4.10.3 A solução deve suportar varreduras programadas de serviços SOAP e REST API.

4.10.4 A solução deve contar com uma API e integração com Jenkins para automação em um ambiente de CI / CD.

4.10.5 A solução deve detectar, identificar, avaliar, rastrear os 10 principais riscos OWASP (Top 10), como injeção de SQL, Cross-site script (XSS), XML External Entity (XXE), autenticação interrompida e configurações incorretas, também ameaças de WASC, vulnerabilidades CWE e CVEs associados em aplicações da web.

4.10.6 A solução deve suportar a capacidade de retesar uma vulnerabilidade específica que foi detectada anteriormente na aplicação web.

4.10.7 A solução deve ter capacidade de encontrar aplicações web aprovadas e não aprovadas em sua rede, gerando um processo contínuo de catalogação e descoberta de aplicações web.

4.10.8 A solução deve gerar tags para facilitar a localização e o uso de ativos de aplicações web encontrados.

4.10.9 A solução deve permitir que se faça a varredura de grandes aplicações da web usando um mecanismo de varredura progressiva, que deve permitir a varredura em estágios incrementais e evitar quaisquer restrições que possam surgir ao tentar fazer a varredura de um aplicativo de uma vez.

4.10.10 A solução deve definir a hora exata de início e duração das verificações.

4.10.11 A solução deve permitir gerenciar várias varreduras de aplicações web, combinando vários scanners para acelerar o processo e obter resultados mais rapidamente.

4.10.12 A solução deve permitir integração nativa com uma das seguintes ferramentas de WAF: F5, Fortinet, Imperva, Citrix NetScaler

4.10.13 A solução deve consolidar os dados de varredura automatizada da solução com dados

de ferramentas que permitem a avaliação manual de vulnerabilidades por meio do Burp Suite e Bugcrowd, para uma visão unificada de vulnerabilidades de aplicações web detectadas automática e manualmente.

4.10.14 A solução deve fornecer relatórios resumidos e de varredura do site que podem ser exportados para os formatos HTML e PDF.

4.10.15 A solução deve oferecer suporte à criação de escopos e funções definidos pelo usuário e permitir que as permissões apropriadas sejam atribuídas a cada função.

5 Entrega

5.1 Após a assinatura do contrato, as licenças devem estar disponíveis para verificação no site do fabricante, em nome da Assembleia Legislativa de Santa Catarina, bem como o acesso a plataforma em nuvem do fabricante para gestão de vulnerabilidades em até 15 (quinze) dias corridos

5.2 Não é necessária a entrega de mídias físicas, bastando a disponibilização de link funcional para acesso a plataforma.

5.3 As licenças, instruções e demais itens necessários para a correta disponibilização da solução, podem ser enviados por meio eletrônico a ser acordado.

6 Qualificação Técnica

6.1 Será exigida a apresentação de, no mínimo, 01 (um) atestado de capacidade Técnico operacional, em nome da proponente, expedido por uma pessoa jurídica de direito público ou privado, comprovando a experiência no fornecimento prestação de serviços de implementação de ambientes utilizando este produto, dentro do território nacional;

6.2 Fica dispensada de apresentação de atestado de capacidade técnica a PROPONENTE que subcontratar o fabricante da solução para a execução dos serviços exigidos no presente Edital. Neste caso a PROPONENTE deverá apresentar declaração do fabricante para comprovação do presente item

7 Treinamento

7.1 A contratada deverá disponibilizar um treinamento da solução contratada no formato E-Learning ou presencial para no mínimo 2 (duas) pessoas, com carga horária mínima de 24 (vinte e quatro) horas e realização em horário comercial.

7.2 O instrutor poderá ser um funcionário da fabricante ou da contratada desde que possua a certificação homologada pela fabricante

7.3 Em caso de treinamento presencial ele deverá ser realizado em horário de expediente da ALESC (07:00 as 19:00 horas) de segunda a sexta-feira excluindo-se sábados, domingos e feriados municipais, estaduais e nacionais, conforme cronograma a ser estabelecido de comum acordo entre as partes;

7.4 Ao final do treinamento a contratada deverá emitir um certificado de conclusão informando a carga horária e os softwares utilizados no mesmo;

8 Suporte

8.1 - Os serviços de manutenção e suporte por 36 meses, incluindo correções, atualizações e suporte técnico telefônico ou website, necessário ao perfeito funcionamento da solução, deverão ser prestados de forma integral pelo FABRICANTE do software.

- 8.2** Por serviços suporte técnico telefônico ou website, entende-se a disponibilização de canal de comunicação com o FABRICANTE do software para esclarecimento de dúvidas técnicas relacionadas aos produtos adquiridos e abertura de chamados de problemas ou dúvidas, sem custos adicionais para a CONTRATANTE. Tais serviços deverão estar disponíveis 24x7x365 (vinte quatro horas por dia, sete dias por semana, 365 dias por ano).
- 8.3** Por atualização entende-se a possibilidade de utilização de novas versões dos softwares adquiridos que forem disponibilizadas pelo FABRICANTE durante o período de cobertura do contrato.
- 8.4** Suporte com janela de abertura de chamado 24 horas, 7 dias na semana, 365 dias por ano, com tempo de atendimento de até duas (02) horas para chamados críticos, prestado por Analistas de Suporte Remoto;
- 8.5** Todos os chamados serão atendidos e gerenciados pela central de atendimento do fabricante da solução de software através de número telefônico 0800 ou equivalente de ligação gratuita, em língua portuguesa, fornecendo o número, data e hora da abertura do chamado;
- 8.6** Não deverá haver qualquer limitação para o número de solicitações de suporte.

9 Obrigações da contratada

- 9.1** Manter as condições de habilitação e qualificação apresentadas na licitação, durante toda a execução do Contrato;
- 9.2** Dar fiel execução ao objeto contratado, nos moldes da proposta apresentada, nos prazos previstos neste TR,
- 9.3** Prestar informações e os esclarecimentos que venham a ser solicitados pelo CONTRATANTE, durante o período de vigência;
- 9.4** Atender prontamente a quaisquer exigências da fiscalização inerentes ao objeto do Contrato, sem ônus adicionais para a ALESC;
- 9.5** Aceitar, nas mesmas condições contratadas, os acréscimos ou supressões que se fizerem necessários, até o limite de 25% (vinte e cinco por cento) do valor atualizado do contrato;

10 Obrigações do contratante

- 10.1** Designar fiscais para o contrato que farão anotação em ficha própria das faltas e defeitos ocorridos (se houver), os quais deverão ser sanados pela licitante contratada dentro dos prazos previstos neste TR,
- 10.2** Recusar os produtos e serviços que não estejam de acordo com as especificações constantes deste TR;
- 10.3** Cumprir todas as demais obrigações constantes no TR,

11 Sanções administrativas

- 11.1** A Alesc poderá aplicar à licitante vencedora as seguintes penalidades previstas no art. 156 da Lei nº 14.133/21, em caso de inexecução total ou parcial do objeto:
- 11.1.1** Advertência;

11.1.2 12.1.2 - Multa de 1% (um por cento) do valor da proposta para cada dia ou fração de atraso na execução do serviço;

11.1.3 12.1.3 - Multa de até 10% (dez por cento) do valor remanescente em caso de desistência na execução do serviço;

11.2 - Sem prejuízo das sanções previstas no art. 156 da Lei nº 14.133/21, a licitante adjudicatária ficará sujeita às seguintes penalidades:

11.2.1 Até 10% (dez por cento) do valor do Contrato atualizado pela execução do serviço desconforme com o especificado;

11.2.2 1% (um por cento) ao dia do valor do Contrato atualizado pela não substituição dos itens e/ou serviços recusados pela ALESC, no prazo estipulado, até o limite de 10% (dez por cento);

11.2.3 Até 10% (dez por cento) do valor do Contrato atualizado pelo descumprimento Termo de Referência 0672320 SEI 23.0.000007886-7 / pg. 6 dos prazos e condições previstos no Edital, exceto nos casos previstos dos itens acima;

11.3 - Havendo justificativa plausível por parte da empresa (motivo de força maior ou comprovado impedimento), respectiva multa poderá deixar de ser aplicada, cuja justificativa poderá ou não ser aceita pela Administração.

11.4 A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança não isentará a obrigação de indenizar eventuais perdas e danos.

12 Pagamento

12.1 Proposta de preços

12.1.1 A proposta de preços deverá conter, obrigatoriamente, os preços unitários e totais de cada item

12.1.2 Os preços deverão estar indicados em moeda nacional e serão considerados completos, incluídas quaisquer vantagens, abatimentos, impostos, taxas e contribuições sociais, obrigações trabalhistas, previdenciárias, fiscais e comerciais, que eventualmente, incidam sobre a operação; ou, ainda despesas com transporte ou terceiros, que ocorrerão por conta da Licitante vencedora.

12.1. Serão considerados, para fins de julgamento, os valores constantes nos preços até, no máximo duas casas decimais após a vírgula.

12.2 Pagamento e reajuste anual

12.2.1 O pagamento se dará conforme tabela abaixo, após a emissão de “Termo de Recebimento Definitivo” por parte do Gestor Técnico, de acordo com os prazos contratuais estabelecidos.

Solução de Gestão de Vulnerabilidades		
Item	Descrição	Pagamento
1	Solução de gerenciamento de vulnerabilidades, detecção e resposta	Único
2	Solução de gerenciamento de patches	Único
3	Assinatura de digitalização de aplicativos Web (Web Scanning)	Único
4	Suporte técnico	Mensal

5	Treinamento oficial para operação e troubleshooting	Único
---	---	-------

13 Dotação Orçamentária

13.1 Em face da recomendada segregação de funções, a dotação orçamentária deve ficar por conta da área competente.

14 Especificações Gerais

14.1 Local de Entrega: Assembleia Legislativa do Estado de Santa Catarina - Unidade Administrativa - AV. Mauro Ramos, 300, CEP: 88020-300 - Florianópolis - Santa Catarina;

14.2 Certificação: A empresa deverá ser certificada como distribuidor oficial da marca oferecida, comprovando através de carta do fabricante especificamente para esse edital.

15 Acompanhamento da Entrega

15.1 - O setor responsável pelo recebimento, fiscalização e aceite será a Coordenadoria de Redes.

ANEXO II

EDITAL DE PREGÃO ELETRÔNICO Nº 024/2024

PLANILHA DE VALORES MÁXIMOS ADMISSÍVEIS

Item	Descrição	Unid.	CATMAT	Qtidade	Valor unitário (R\$)	Subtotal (R\$)	Intervalo mínimo de lances (R\$)
1	Assinatura de digitalização de aplicativos web (web scanning)	UN	27081	1	432.515,55	432.515,55	
2	Solução de gerenciamento de patches	UN	27081	1	171.252,40	171.252,40	
3	Solução de gerenciamento de vulnerabilidades, detecção e resposta	UN	27081	1	178.023,82	178.023,82	

4	Suporte técnico (solução de gestão de vulnerabilidades)	SV	27081	36	2.500,00	90.000,00	
5	Treinamento oficial para operação e troubleshooting	SV	27081	1	25.000,00	25.000,00	
Valor Máximo Admissível (R\$)						896.791,77	

ANEXO III

EDITAL DE PREGÃO ELETRÔNICO Nº 024/2024

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: _____

1. A presente proposta tem como objeto a contratação de ferramenta para gerenciamento de vulnerabilidades em servidores, estações de trabalho e ativos de rede, incluindo instalação, configuração, suporte garantia e treinamento, em conformidade com as especificações, quantidades e demais condições definidas no edital e seus anexos.

Item	Descrição	Unid.	Qtidade	Valor unitário (R\$)	Subtotal (R\$)
1	Assinatura de digitalização de aplicativos web (web scanning)	UN	1		
2	Solução de gerenciamento de patches	UN	1		
3	Solução de gerenciamento de vulnerabilidades, detecção e resposta	UN	1		

4	Suporte técnico (solução de gestão de vulnerabilidades)	SV	36		
5	Treinamento oficial para operação e troubleshooting	SV	1		
Valor Total (R\$)					

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 de 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 N° 024/2024

DECLARAÇÃO DE CUMPRIMENTO DA LEI GERAL DE PROTEÇÃO DE DADOS

LEI N° 13.709/2018

1. 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.

2. As partes se comprometem a manter sigilo e confidencialidade de todas as informações – em especial os dados pessoais e os dados pessoais sensíveis – repassados em decorrência da execução contratual, em consonância com o disposto na Lei n. 13.709/2018, sendo vedado o repasse das informações a outras empresas ou pessoas, salvo aquelas decorrentes de obrigações legais ou para viabilizar o cumprimento do edital/instrumento contratual.

3. As partes responderão administrativa e judicialmente, em caso de causarem danos patrimoniais, morais, individual ou coletivo, aos titulares de dados pessoais, repassados em decorrência da execução contratual, por inobservância à LGPD.

4. Em atendimento ao disposto na Lei n. 13.709/2018 - Lei Geral de Proteção de Dados Pessoais(LGPD), o Contratante, para a execução do serviço objeto deste edital, terá acesso aos dados pessoais dos representantes da licitante/contratada/detentora da ata, tais como: número do CPF e do RG, endereço eletrônico, cópia do documento de identificação.

5. A licitante/contratada/detentora da ata, declara que tem ciência da existência da Lei Geral de Proteção de Dados (LGPD) e, se compromete a adequar todos os procedimentos internos ao disposto na legislação, com intuito de proteção dos dados pessoais repassados pelo Contratante.

6. A licitante/contratada/detentora da ata, fica obrigada a comunicar ao Contratante, em até 24 (vinte e quatro) horas, qualquer incidente de acessos não autorizados aos dados pessoais, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito que possa vir a causar risco ou dano relevante aos Titulares de Dados Pessoais, apresentando as informações descritas nos incisos do § 1º do art. 48 da LGPD, cabendo ao Contratante as demais obrigações de comunicação previstas no referido artigo.

Florianópolis/SC ____ de ____ de 2024.

Representante legal

(Assinatura e carimbo da empresa)

ANEXO V

EDITAL DE PREGÃO ELETRÔNICO Nº 024/2024

DECLARAÇÃO DE QUE ATENDE ÀS LEIS ESTADUAIS NºS 10.732/98 e 16.003/13

Para atendimento ao disposto no Edital de Pregão Eletrônico nº 024/2024, promovida pela ALESC, a empresa _____ estabelecida na Rua _____ nº _____, Bairro _____, Cidade _____/_____, inscrita no CNPJ/MF sob nº _____._____._____/_____-_____, por intermédio de seu representante legal, DECLARA que atende às exigências das Leis estaduais nºs 10.732, de 07/04/1998, e 16.003, de 25/04/2013, esta última regulamentada pelo Decreto estadual nº 1.694, de 23/08/2013.

DECLARA, ainda, que se compromete a fornecer os comprovantes necessários quando assim solicitados pela **ALESC**.

Florianópolis/SC ____ de ____ de 2024

Assinatura do Responsável

Carimbo da Empresa

ANEXO VI

EDITAL DE PREGÃO ELETRÔNICO Nº 024/2024

MINUTA DO CONTRATO

CONTRATO Nº/....., QUE CELEBRAM ENTRE SI A
ASSEMBLEIA LEGISLATIVA DO ESTADO DE SANTA
CATARINA E A EMPRESA
.....

A ASSEMBLEIA LEGISLATIVA DO ESTADO DE SANTA CATARINA, inscrita no CNPJ sob o nº 83.599.191/0001-87, com sede na Rua Doutor Jorge Luz Fontes nº 310, na cidade de Florianópolis/SC, CEP 88020-900, neste ato representada por seu Diretor-Geral, Alexandre Lencina Fagundes, e por seu Diretor de Tecnologia e Informações, Ami Nadabe Ozelame, doravante denominada CONTRATANTE, e o(a), inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, em doravante designada contratada, neste ato representado(a) por (nome e função na contratada), conforme atos constitutivos da empresa **OU** procuração apresentada nos autos, tendo em vista o que consta no Processo SEI nº 23.0.000030861-7 e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais normas aplicáveis, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico nº 024/2024, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1. O objeto do presente instrumento é a contratação de ferramenta para gerenciamento de vulnerabilidades em servidores, estações de trabalho e ativos de rede, incluindo instalação, configuração, suporte garantia e treinamento, nas condições estabelecidas no Termo de Referência.

1.2. Objeto da contratação:

Item	Descrição	Unid.	Qtidade	Valor unitário (R\$)	Subtotal (R\$)
1	Assinatura de digitalização de aplicativos web (web scanning)	UN	1		
2	Solução de gerenciamento de patches	UN	1		
3	Solução de gerenciamento de vulnerabilidades, detecção e resposta	UN	1		
4	Suporte técnico (solução de gestão de vulnerabilidades)	SV	36		
5	Treinamento oficial para operação e troubleshooting	SV	1		
Valor Total (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 dos [artigos 106 e 107 da Lei nº 14.133, de 2021.](#)

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

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

2.4. 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.

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

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

3.1. O regime de execução contratual, os modelos de gestão e de execução, assim como os prazos e condições de conclusão, entrega, observação e recebimento do objeto constam no Termo de Referência, anexo a este Contrato.

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. É permitida à licitante subcontratar o fabricante da solução para a execução dos serviços exigidos no presente Edital.

4.2. Em qualquer hipótese de subcontratação, permanece a responsabilidade integral da contratada pela perfeita execução contratual, cabendo-lhe realizar a supervisão e coordenação das atividades do subcontratado, bem como responder perante o contratante pelo rigoroso cumprimento das obrigações contratuais correspondentes ao objeto da subcontratação.

4.3. É vedada a subcontratação de pessoa física ou jurídica, se aquela ou os dirigentes desta mantiverem vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na contratação ou atue na fiscalização ou na gestão do contrato, ou se deles forem cônjuge, companheiro ou parente em linha reta, colateral, ou por afinidade, até o terceiro grau.

CLÁUSULA QUINTA – PREÇO

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

5.2. 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.

CLÁUSULA SEXTA – PAGAMENTO

6.1. O pagamento se dará conforme tabela abaixo, após a emissão de “Termo de Recebimento Definitivo” por parte do Fiscal do Contrato, de acordo com os prazos contratuais estabelecidos.

Item	Descrição	Pagamento
1	Assinatura de digitalização de aplicativos web (web scanning)	Pagamento único
2	Solução de gerenciamento de patches	Pagamento único
3	Solução de gerenciamento de vulnerabilidades, detecção e resposta	Pagamento único
4	Suporte técnico (solução de gestão de vulnerabilidades)	Pagamento Mensal (36 meses)
5	Treinamento oficial para operação e troubleshooting	Pagamento único

6.2. Não será emitido aceite parcial para nenhum destes itens.

6.3. Quando aplicável, o valor anual corresponde a parte proporcional do valor global contratado.

6.4. O pagamento será realizado após a apresentação das notas fiscais e certidões de regularidade fiscal exigidas em lei.

6.5. A nota de cobrança emitida pela CONTRATADA deverá ser atestada pelo gestor de contrato e encaminhada para a área financeira efetuar o pagamento.

6.6. 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.

6.7. 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.

6.8. 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).

6.9. 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 de 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.

6.10. 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.

6.11. 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.

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

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

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

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

6.14. 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.

6.15. 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.

6.16. 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.

6.17. 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.

CLÁUSULA SÉTIMA – REAJUSTE

7.1. Após o interregno de um ano, e independentemente de pedido da contratada, os preços iniciais serão reajustados, mediante a aplicação, pelo contratante, do Índice Nacional de Preços ao Consumidor Amplo – IPCA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.

7.2. O prazo de um ano será contado a partir do dia 27/11/2023, data da consolidação da Pesquisa de Preços

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

7.4. 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.

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

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

CLÁUSULA OITAVA – OBRIGAÇÕES DA CONTRATANTE

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

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

8.3. 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;

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

8.5. A fiscalização ficará a cargo do titular da Coordenadoria de Redes ou servidor por este designado.

8.6. 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;

8.7. 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;

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

8.9. 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.

8.10. 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.

8.11. Notificar os emitentes das garantias quanto ao início de processo administrativo para apuração de descumprimento de cláusulas contratuais.

8.12. Comunicar a contratada na hipótese de posterior alteração do projeto pelo Contratante, no caso [do art. 93, §2º, da Lei nº 14.133, de 2021](#).

8.13. 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 NONA – OBRIGAÇÕES GERAIS DA CONTRATADA

9.1. A contratada deve 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, observando, ainda, as obrigações a seguir dispostas:

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

9.1.2. 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;

9.1.3. 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;

9.1.4. 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;

9.1.5. 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](#);

9.1.6. 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;

9.1.7. 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.

9.1.8. 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.

9.1.9. 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.

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

9.1.11. 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.

9.1.12. 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.

9.1.13. 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;

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

9.1.15. 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;

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

9.1.17. 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](#);

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

CLÁUSULA DÉCIMA – TREINAMENTO

10.1. A contratada deverá disponibilizar um treinamento da solução contratada no formato E-Learning ou presencial para no mínimo duas pessoas, com carga horária mínima de 24 (vinte e quatro) horas e realização em horário comercial.

10.2. O instrutor poderá ser um funcionário da fabricante ou da contratada desde que possua a certificação homologada pela fabricante.

10.3. Em caso de treinamento presencial ele deverá ser realizado em horário de expediente da ALESC (07:00 as 19:00 horas) de segunda a sexta-feira excluindo-se sábados, domingos e feriados municipais, estaduais e nacionais, conforme cronograma a ser estabelecido de comum acordo entre as partes.

10.4. Ao final do treinamento a contratada deverá emitir um certificado de conclusão informando a carga horária e os softwares utilizados no mesmo.

CLÁUSULA DÉCIMA PRIMEIRA – 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 o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

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.

11.12. Os contratos e convênios de que trata o [§ 1º do art. 26 da LGPD](#) deverão ser comunicados à autoridade nacional.

12. CLÁUSULA DÉCIMA SEGUNDA – SUPORTE

12.1. Os serviços de manutenção e suporte por 36 meses, incluindo correções, atualizações e suporte técnico telefônico ou website, necessário ao perfeito funcionamento da solução, deverão ser prestados de forma integral pelo FABRICANTE do software.

12.2. Por serviços suporte técnico telefônico ou website, entende-se a disponibilização de canal de comunicação com o FABRICANTE do software para esclarecimento de dúvidas técnicas relacionadas aos produtos adquiridos e abertura de chamados de problemas ou dúvidas, sem custos adicionais para a CONTRATANTE. Tais serviços deverão estar disponíveis 24x7x365 (vinte quatro horas por dia, sete dias por semana, 365 dias por ano).

12.3. Por atualização entende-se a possibilidade de utilização de novas versões dos softwares adquiridos que forem disponibilizadas pelo FABRICANTE durante o período de cobertura do contrato.

12.4. Suporte com janela de abertura de chamado 24 horas, 7 dias na semana, 365 dias por ano, com tempo de atendimento de até duas (02) horas para chamados críticos, prestado por Analistas de Suporte Remoto.

12.5. Todos os chamados serão atendidos e gerenciados pela central de atendimento do fabricante da solução de software através de número telefônico 0800 ou equivalente de ligação gratuita, em língua portuguesa, fornecendo o número, data e hora da abertura do chamado.

12.6. Não deverá haver qualquer limitação para o número de solicitações de suporte.

CLÁUSULA DÉCIMA TERCEIRA – 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 ou 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 contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;

- f) 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:

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

13.2.2. Impedimento de licitar e contratar, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave;

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

13.2.4. Multa:

13.2.4.1. de 1% (um por cento) do valor da proposta para cada dia ou fração de atraso na execução do serviço;

13.2.4.2. de até 10% (dez por cento) do valor remanescente em caso de desistência na execução do serviço;

13.2.5. Sem prejuízo das sanções previstas no art. 156 da Lei nº 14.133/2021, a licitante adjudicatária ficará sujeita às seguintes penalidades:

13.2.5.1. Até 10% (dez por cento) do valor do Contrato atualizado pela execução do serviço desconforme com o especificado;

13.2.5.2. De 1% (um por cento) ao dia do valor do Contrato atualizado pela não substituição dos itens e/ou serviços recusados pela ALESC, no prazo estipulado, até o limite de 10% (dez por cento);

13.2.5.2. Até 10% (dez por cento) do valor do Contrato atualizado pelo descumprimento Termo de Referência (TR), dos prazos e condições previstos no Edital, exceto nos casos previstos dos itens acima;

13.3. Havendo justificativa plausível por parte da empresa (motivo de força maior ou comprovado impedimento), respectiva multa poderá deixar de ser aplicada, cuja justificativa poderá ou não ser aceita pela Administração.

13.4. A multa poderá ser aplicada cumulativamente com as demais sanções, não terá caráter compensatório e a sua cobrança não isentará a obrigação de indenizar eventuais perdas e danos.

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

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

CLÁUSULA DÉCIMA QUARTA – DA EXTINÇÃO CONTRATUAL

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

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

14.3. Quando a não conclusão do contrato referida no item anterior decorrer de culpa da contratada:

- a) ficará ele constituído em mora, sendo-lhe aplicáveis as respectivas sanções administrativas; e
- b) poderá a Administração optar pela extinção do contrato e, nesse caso, adotará as medidas admitidas em lei para a continuidade da execução contratual.

CLÁUSULA DÉCIMA QUINTA – DOTAÇÃO ORÇAMENTÁRIA

15.1. As despesas pertinentes ao objeto do presente Edital correrão à conta da Subação 001369 (Manutenção, serviços e equipamentos de informática), Fonte do Recurso 1.500.100.000 (Recursos Não Vinculados de Impostos - Receita Líquida Disponível - RLD - Fonte Tesouro - EC), Natureza da Despesa 33.90.40.11 (Locação de Softwares); 33.90.40.08 (Manutenção de Softwares); e 33.90.39.48 (Serviços de Seleção e Treinamento) do Orçamento da ALESC.

CLÁUSULA DÉCIMA SEXTA – 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 8.078, de 1990 – Código de Defesa do Consumidor](#) – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SÉTIMA – ALTERAÇÕES

17.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos [arts. 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 (art. 132 da Lei nº 14.133, de 2021).

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 DÉCIMA OITAVA – 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 à 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 DÉCIMA NONA – 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 nº 14.133, de 2021.

CLÁUSULA VIGÉSIMA – 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)

Alexandre Lencina Fagundes
Diretor Geral

Ami Nadabe Ozelame
Diretor de Tecnologia e Informações

CONTRATADA

[Representante Legal]



Documento assinado eletronicamente por **ALEXANDRE RODRIGUES BADOTTI, Coordenador de Licitações e Contratos**, em 16/05/2024, às 17:56, conforme art. 1º, III, "b", da Lei 11.419/2006.



Documento assinado eletronicamente por **ALEXANDRE LENCINA FAGUNDES, Diretor-Geral**, em 18/05/2024, às 06:32, 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 **1263924** e o código CRC **754C9960**.