PREGÃO ELETRÔNICO Nº 0011/2026
CONSÓRCIO INTERMUNICIPAL DE DESENVOLVIMENTO SUSTENTÁVEL DA SERRA GAÚCHA

OBJETO: Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA, conforme condições e exigências estabelecidas neste instrumento.

CALENDÁRIO

DATA DA SESSÃO PÚBLICA: Dia 09/10/2026 às 9 horas (horário de Brasília)
RECEBIMENTO DAS PROPOSTAS: a partir das 08 horas do dia 25/09/2026 até às 08 horas do dia 09/10/2026.
ABERTURA DAS PROPOSTAS: a partir das 08 horas do dia 09/10/2026.
REFERÊNCIA DE TEMPO: horário de Brasília (DF)

LOCAL:
www.pregaobanrisul.com.br

CRITÉRIO DE JULGAMENTO: MENOR PREÇO

DECREMENTO: 1%

MODO DE DISPUTA: ABERTO

AMPLA CONCORRÊNCIA
Tratamento Preferencial ME/EPP

SUMÁRIO

PREGÃO ELETRÔNICO N.º 0011/2026
POR REGISTRO DE PREÇOS
Processo Administrativo nº 031/2026

Torna-se público que o(a) **CONSÓRCIO INTERMUNICIPAL DE DESENVOLVIMENTO SUSTENTÁVEL DA SERRA GAÚCHA – CP – CISGA**, sediado(a) na rua Jacob Ely, 498, sala 5, Centro, na cidade de Garibaldi-RS, realizará licitação, para REGISTRO DE PREÇOS, na modalidade **PREGÃO**, na forma **ELETRÔNICA**, nos termos da Lei nº 14.133, de 1º de abril, do Decreto nº 11.462, de 31 de março de 2023, e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

1.1. Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
1.2. A descrição pormenorizada do item, unidade de fornecimento e quantidades estimadas estão dispostas no Termo de Referência.

2. DO REGISTRO DE PREÇOS

2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam da minuta de Ata de Registro de Preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste certame os interessados cujo ramo de atividade seja compatível com o objeto da licitação e estiverem previamente cadastrados no portal do Fornecedor.RS (https://portaldofornecedor.rs.gov.br/#/home) para credenciamento eletrônico.
3.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluída a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.
3.3. 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.
3.4. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.
3.5. O Termo de Referência, indicará, **se for o caso**, para quais itens a participação será exclusiva para microempresas e empresas de pequeno porte, nos termos do art. 48 da Lei Complementar n.º 123, de 14 de dezembro de 2006.
3.6. A obtenção do benefício a que se refere o item anterior 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.
3.7. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para as sociedades cooperativas mencionadas no artigo 16 da Lei nº 14.133, de 2021, para o agricultor familiar, o produtor rural pessoa física e para o microempreendedor individual - MEI, nos limites previstos da Lei Complementar nº 123, de 2006 e do Decreto n.º 8.538, de 2015.

3.8. Não poderão disputar esta licitação:

3.8.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.8.2. sociedade que desempenhe atividade incompatível com o objeto da licitação;

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

3.8.4. 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;

3.8.5. 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;

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

3.8.7. aquele que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

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

3.8.9. 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;

3.8.10. agente público do órgão ou entidade licitante;

3.8.11. pessoas jurídicas reunidas em consórcio, conforme justificativa encartada no ETP;

3.8.12. organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição.

3.9. Não poderá participar, direta ou indiretamente, da licitação ou da execução do contrato agente público do órgão ou entidade contratante, devendo ser observadas as situações que possam configurar conflito de interesses no exercício ou após o exercício do cargo ou emprego, nos termos da legislação que disciplina a matéria, conforme § 1º do art. 9º da Lei nº 14.133, de 2021.

3.10. O impedimento de que trata o item 3.8.6 será também aplicado ao licitante que atue em substituição a outra pessoa, física ou jurídica, com o intuito de burlar a efetividade da sanção a ela aplicada, inclusive a sua controladora, controlada ou coligada, desde que devidamente comprovado o ilícito ou a utilização fraudulenta da personalidade jurídica do licitante.

3.11. A critério da Administração e exclusivamente a seu serviço, o autor dos projetos e a empresa a que se referem os itens 3.8.4 e 3.8.5 poderão participar no apoio das atividades de planejamento da contratação, de execução da licitação ou de gestão do contrato, desde que sob supervisão exclusiva de agentes públicos do órgão ou entidade.

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

3.13. O disposto nos itens 3.8.4 e 3.8.5 não impede a licitação ou a contratação de serviço que inclua como encargo do contratado a elaboração do projeto básico e do projeto executivo, nas contratações integradas, e do projeto executivo, nos demais regimes de execução.

3.14. Em licitações e contratações realizadas no âmbito de projetos e programas parcialmente financiados por agência oficial de cooperação estrangeira ou por organismo financeiro internacional com recursos do financiamento ou da contrapartida nacional, não poderá participar pessoa física ou jurídica que integre o rol de pessoas sancionadas por essas entidades ou que seja declarada inidônea nos termos da Lei nº 14.133/2021.

3.15. A vedação de que trata o item 3.11 estende-se a terceiro que auxilie a condução da contratação na qualidade de integrante de equipe de apoio, profissional especializado ou funcionário ou representante de empresa que preste assessoria técnica.

4. DO ORÇAMENTO ESTIMADO

4.1. O orçamento estimado da presente contratação será de caráter sigiloso.
4.2. Para fins do disposto no item anterior, o orçamento estimado para a contratação não será tornado público antes de definido o resultado do julgamento das propostas.
4.3. O caráter sigiloso do orçamento estimado para a contratação não prevalecerá para os órgãos de controle interno e externo.

5. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

5.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas lances e de julgamento.
5.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com a descrição do objeto ofertado, o preço ou o percentual de desconto, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.
5.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, antes do envio da proposta, que:

5.3.1. que tem pleno conhecimento e atende a todas as exigências de habilitação e especificações técnicas previstas no edital;
5.3.2. o fornecedor enquadrado como microempresa, empresa de pequeno porte ou sociedade cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no artigo 3° da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos §§ 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021.

5.4. Caso não seja utilizada a faculdade prevista no subitem 5.3.2, será considerado que a licitante optou por renunciar aos benefícios previstos na Lei Complementar nº 123/06.
5.5. Não poderá se beneficiar do tratamento jurídico diferenciado estabelecido nos arts. 42 a 49 da Lei Complementar nº 123, de 2006, a pessoa jurídica:

5.5.1. de cujo capital participe outra pessoa jurídica;
5.5.2. que seja filial, sucursal, agência ou representação, no País, de pessoa jurídica com sede no exterior;
5.5.3. de cujo capital participe pessoa física que seja inscrita como empresário ou seja sócia de outra empresa que receba tratamento jurídico diferenciado nos termos da Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;
5.5.4. cujo titular ou sócio participe com mais de 10% (dez por cento) do capital de outra empresa não beneficiada pela Lei Complementar nº 123, de 2006, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;
5.5.5. cujo sócio ou titular seja administrador ou equiparado de outra pessoa jurídica com fins lucrativos, desde que a receita bruta global ultrapasse o limite de que trata o inciso II do art. 3º da referida lei;
5.5.6. constituída sob a forma de cooperativas, salvo as de consumo;
5.5.7. que participe do capital de outra pessoa jurídica;
5.5.8. que exerça atividade de banco comercial, de investimentos e de desenvolvimento, de caixa econômica, de sociedade de crédito, financiamento e investimento ou de crédito imobiliário, de corretora ou de distribuidora de títulos, valores mobiliários e câmbio, de empresa de

arrendamento mercantil, de seguros privados e de capitalização ou de previdência complementar;

5.5.9. resultante ou remanescente de cisão ou qualquer outra forma de desmembramento de pessoa jurídica que tenha ocorrido em um dos 5 (cinco) anos-calendário anteriores;

5.5.10. constituída sob a forma de sociedade por ações;

5.5.11. cujos titulares ou sócios guardem, cumulativamente, com o contratante do serviço, relação de pessoalidade, subordinação e habitualidade.

5.6. A falsidade das declarações de que tratam os itens 3.3.1 e 3.3.2 sujeitará o licitante às sanções previstas na Lei nº 14.133, de 2021, e neste Edital.

5.7. Os licitantes poderão retirar ou substituir a proposta até a data e horário previsto para o término do recebimento de propostas.

5.8. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após o a julgamento da proposta.

5.9. Caberá ao licitante interessado em participar da licitação acompanhar as operações no sistema eletrônico durante o processo licitatório e se responsabilizar pelo ônus decorrente da perda de negócios diante da inobservância de mensagens emitidas pela Administração ou de sua desconexão.

5.10. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

6. DO PREENCHIMENTO DA PROPOSTA

6.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos, **se aplicável**:

6.1.1. valor unitário, marca e modelo/fabricante.

6.2. A Proposta escrita, anexada no sistema eletrônico, deve conter as seguintes informações:

6.2.1. número do item (conforme apêndice I do Termo de Referência);

6.2.2. descrição do item (conforme apêndice I do Termo de Referência);

6.2.3. indicação de Marca e fabricante de cada item proposto (a licitante deverá informar apenas **UMA marca/fabricante** na proposta e também no cadastro no sistema).

6.2.4. quantidade Estimada, quantitativo estabelecido no Termo de Referência;

6.2.5. valor unitário ofertado por cada item em moeda corrente nacional, com o máximo de 02 (duas) casas decimais após a vírgula;

6.2.6. valor total por cada item (valor da unidade multiplicado pela quantidade estimada do item), em moeda corrente nacional, com o máximo de 02 (duas) casas decimais após a vírgula;

6.2.7. indicação do valor total da proposta, em moeda corrente nacional, em algarismo e por extenso;

6.2.8. razão social completa da empresa e CNPJ;

6.2.9. endereço atualizado;

6.2.10. telefone e e-mail;

6.2.11. nome da pessoa indicada como contato e da responsável por assinar o contrato; e

6.2.12. dados bancários.

6.2.13. a proposta deverá estar devidamente assinada pelo sócio proprietário da empresa ou seu representante legal, ou ainda por seu representante convencional (procurador), desde que seja anexada a respectiva procuração com poderes específicos para este fim.

6.3. Todas as especificações do objeto contidas na proposta vinculam o licitante.

6.4. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.

6.5. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
6.6. Todas as informações lançadas durante o preenchimento dos campos no sistema eletrônico devem estar rigorosamente de acordo com as da proposta anexada no sistema.
6.7. Os preços ofertados, tanto na proposta inicial quanto na etapa de lances, serão de exclusiva responsabilidade do licitante, não lhe assistindo o direito de pleitear qualquer alteração sob alegação de erro, omissão ou qualquer outro pretexto.
6.8. A(s) detentora(s) da Ata de Registro de Preços deverá(ão) fornecer qualquer quantidade solicitada, desde que não supere as quantidades estimadas dispostas no Termo de Referência, não podendo, portanto, estipular em sua proposta de preços ou por outro qualquer meio de comunicação cota mínimas ou máximas para remessa do(s) produto(s), sob pena de incidência das respectivas sanções.
6.9. Não será admitida a previsão de preços diferentes em razão de local de prestação do serviço ou qualquer outro motivo.
6.10. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
6.11. No regime de incidência não-cumulativa de PIS e COFINS, a cotação adequada será a que corresponde à média das alíquotas efetivamente recolhidas pela empresa, comprovada, a qualquer tempo, por documentos de Escrituração Fiscal Digital da Contribuição (EFD-Contribuições) para o PIS/PASEP e COFINS dos últimos 12 (doze) meses anteriores à apresentação da proposta, ou por outro meio hábil.
6.12. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
6.13. A apresentação das propostas implica obrigatoriedade do cumprimento das disposições nelas contidas, em conformidade com o que dispõe o Termo de Referência, assumindo o proponente o compromisso de executar o objeto licitado nos seus termos, bem como de fornecer os materiais, equipamentos, ferramentas e utensílios necessários, em quantidades e qualidades adequadas à perfeita execução contratual, promovendo, quando requerido, sua substituição.
6.14. O prazo de validade da proposta não será inferior a 60 (sessenta) dias**,** a contar da data de sua apresentação.
6.15. O descumprimento, pelos contratados, das regras supramencionadas pode ensejar a responsabilização pelo Tribunal de Contas do Estado e, após o devido processo legal, gerar as seguintes consequências: assinatura de prazo para a adoção das medidas necessárias ao exato cumprimento da lei, nos termos do art. 71, inciso IX, da Constituição; ou condenação dos agentes públicos responsáveis e da empresa contratada ao pagamento dos prejuízos ao erário, caso verificada a ocorrência de superfaturamento por sobrepreço na execução do contrato.

7. DA ABERTURA DA SESSÃO, CLASSIFICAÇÃO DAS PROPOSTAS E FORMULAÇÃO DE LANCES

7.1. A abertura da presente licitação dar-se-á automaticamente em sessão pública, por meio de sistema eletrônico, na data, horário e local indicados neste Edital.
7.2. Os licitantes poderão retirar ou substituir a proposta, anteriormente inserida no sistema, até a data limite estipulada para o recebimento das propostas.
7.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.
7.4. Iniciada a etapa competitiva, os licitantes deverão encaminhar lances exclusivamente por meio de sistema eletrônico, sendo imediatamente informados do seu recebimento e do valor consignado no registro.
7.5. O lance deverá ser ofertado pelo valor total do lote.
7.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

7.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
7.8. O intervalo mínimo de diferença de valores ou percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação à proposta que cobrir a melhor oferta deverá ser de 1 (um) por cento.
7.9. O modo de disputa adotado por esta Administração é o "aberto", sendo que na fase de disputas os licitantes apresentarão lances públicos e sucessivos, com prorrogações.
7.10. A etapa de lances da sessão pública terá duração de dez minutos e, após isso, será prorrogada automaticamente pelo sistema quando houver lance ofertado nos últimos dois minutos do período de duração da sessão pública.
7.10.1. A prorrogação automática da etapa de lances, de que trata o subitem anterior, será de dois minutos e ocorrerá sucessivamente sempre que houver lances enviados nesse período de prorrogação, inclusive no caso de lances intermediários;
7.10.2. Não havendo novos lances na forma estabelecida nos itens anteriores, a sessão pública encerrar-se-á automaticamente, e o sistema ordenará e divulgará os lances conforme a ordem final de classificação, sem prejuízo da aplicação da margem de preferência e do desempate ficto, conforme disposto neste edital, quando for o caso;
7.10.3. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), o pregoeiro, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações;
7.10.4. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.
7.11. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
7.12. Em disputa aberta serão aceitos pelo sistema dois lances iguais, sendo que o critério desempate automático será a hora de registro do lance no sistema eletrônico.
7.13. 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.
7.14. Quando a desconexão do sistema eletrônico para o pregoeiro persistir por tempo superior a dez minutos, a sessão pública será suspensa e reiniciada somente após decorridas vinte e quatro horas da comunicação do fato pelo Pregoeiro aos participantes, no sítio eletrônico utilizado para divulgação.
7.15. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
7.16. Consideram-se empatadas as propostas apresentadas pelas Microempresas e Empresas de Pequeno Porte que estiverem no limite de até 5 % (cinco por cento) superiores à proposta melhor classificada, desde que esta não seja Microempresa ou Empresa de Pequeno Porte.
7.17. Ocorrendo o empate nos termos da Lei Complementar Federal nº 123/2006, a Microempresa e Empresa de Pequeno Porte melhor classificada poderá apresentar proposta inferior à proposta de menor preço apurada no certame, no prazo máximo de 5 (cinco) minutos, contados após a comunicação automática e abertura na plataforma de pregão, sob pena de preclusão.
7.18. No caso de desistência ou não manifestação do prazo estabelecido pela Microempresa ou da Empresa de Pequeno Porte melhor classificada serão convocadas as remanescentes de mesmo enquadramento empresarial que se encontrem na situação de empate, no intervalo de até 5% (cinco por cento) na ordem de classificação para o exercício de mesmo direito.
7.19. Na hipótese de não haver mais empresas de mesmo enquadramento empresarial, a melhor classificada é a licitante que originalmente apresentou o melhor lance.
7.20. A obtenção do benefício a que se refere o item anterior 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.

7.21. Só poderá haver empate entre propostas iguais (não seguidas de lances).

7.22. Havendo eventual empate entre propostas, o critério de desempate será aquele previsto no art. 60 da Lei nº 14.133, de 2021, nesta ordem:

7.22.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;

7.22.2. avaliação do desempenho contratual prévio dos licitantes, para a qual deverão preferencialmente ser utilizados registros cadastrais para efeito de atesto de cumprimento de obrigações previstos nesta Lei;

7.22.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;

7.22.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

7.23. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:

7.23.1. empresas estabelecidas no território do Estado ou do Distrito Federal do órgão ou entidade da Administração Pública estadual ou distrital licitante ou, no caso de licitação realizada por órgão ou entidade de Município, no território do Estado em que este se localize;

7.23.2. empresas brasileiras;

7.23.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

7.23.4. empresas que comprovem a prática de mitigação, nos termos da Lei nº 12.187, de 29 de dezembro de 2009.

7.24. Esgotados todos os demais critérios de desempate previstos em lei, a escolha do licitante vencedor ocorrerá por sorteio, em ato público, para o qual todos os licitantes serão convocados, vedado qualquer outro processo.

7.25. Em caso de licitação com cota reservada para ME/EPP:

7.25.1. na hipótese de não haver vencedora para a cota reservada, esta poderá ser adjudicada à vencedora da cota universal ou, diante de sua recusa, às licitantes remanescentes, desde que pratiquem o preço da primeira colocada da cota universal, quando aplicável;

7.25.2. se a mesma licitante vencer a cota reservada e a cota universal, a contratação das cotas deverá ocorrer pelo menor preço;

7.25.3. o município dará prioridade de aquisição do objeto das cotas reservadas, quando for o caso, ressalvados os casos em que a cota reservada for inadequada para atender as quantidades ou as condições do pedido, justificadamente.

7.26. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo ou inferior ao desconto definido para a contratação, o pregoeiro/Agente de contratação poderá negociar condições mais vantajosas.

7.26.1. a negociação poderá ser feita com os demais licitantes, segundo a ordem de classificação inicialmente estabelecida, quando o primeiro colocado, mesmo após a negociação, for desclassificado em razão de sua proposta permanecer acima do preço máximo definido pela Administração;

7.26.2. a negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

7.27. Após a negociação do preço, o Pregoeiro/Agente de Contratação/Comissão iniciará a fase de aceitação e julgamento da proposta.

8. DA FASE DE JULGAMENTO

8.1. O Pregoeiro/Agente de Contratação/Comissão solicitará ao licitante mais bem classificado que, no prazo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada dos documentos complementares previstos abaixo:

a) **PROPOSTA ADEQUADA AO ÚLTIMO LANCE OFERTADO após a negociação realizada, que deverá estar de acordo com as diretrizes do item 6 "DO PREENCHIMENTO DA PROPOSTA" e Termo de Referência, em anexo.**

   a. A proposta deverá estar devidamente assinada pelo sócio proprietário da empresa ou seu representante legal, ou ainda por seu representante convencional (procurador), desde que seja anexada a respectiva procuração com poderes específicos para este fim.

b) **DECLARAÇÃO DE QUE SUA PROPOSTA ECONÔMICA COMPREENDE A INTEGRALIDADE DOS CUSTOS** para atendimento dos direitos trabalhistas assegurados na constituição federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas, bem como a integralidade dos custos para a entrega do objeto.

8.2. O pregoeiro verificará se o licitante provisoriamente classificado em primeiro lugar atende às condições de participação no certame, conforme previsto no art. 14 da Lei nº 14.133/2021, legislação correlata e no item 3.8 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

8.2.1. Cadastro Nacional de Empresas Inidôneas e Suspensas - CEIS, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/ceis); e

8.2.2. Cadastro Nacional de Empresas Punidas – CNEP, mantido pela Controladoria-Geral da União (https://www.portaltransparencia.gov.br/sancoes/cnep).

8.3. A consulta aos cadastros será realizada em nome da empresa licitante e também de seu sócio majoritário, por força da vedação de que trata o artigo 12 da Lei n° 8.429, de 1992.

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

8.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação;

8.4. Constatada a existência de sanção, o licitante será reputado inabilitado, por falta de condição de participação.

8.5. Verificadas as condições de participação e de utilização do tratamento favorecido, o pregoeiro examinará a proposta classificada em primeiro lugar quanto à adequação ao objeto e à compatibilidade do preço em relação ao máximo estipulado para contratação neste Edital e em seus anexos.

8.6. Será desclassificada a proposta vencedora que:

8.6.1. contiver vícios insanáveis;

8.6.2. não obedecer às especificações técnicas contidas no Edital e seus anexos;

8.6.3. **apresentar preços inexequíveis, preços que permanecerem acima do preço máximo definido para a contratação**;

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

8.6.5. apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

8.7. No caso de bens e serviços em geral, é indício de inexequibilidade das propostas valores inferiores a 50% (cinquenta por cento) do valor orçado pela Administração.

8.8. A inexequibilidade, na hipótese de que trata o caput, só será considerada após diligência do pregoeiro, que comprove:

8.8.1. que o custo do licitante ultrapassa o valor da proposta; e

8.8.2. inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

8.9. Além do critério econômico, poderá ser considerado inexequível o projeto que não apresente condições técnicas, metodológicas ou de equipe suficientes para a execução do objeto, conforme avaliação do pregoeiro e manifestação da área técnica requisitante.
8.10. Se houver indícios de inexequibilidade da proposta de preço, ou em caso da necessidade de esclarecimentos complementares, poderão ser efetuadas diligências, para que a empresa comprove a exequibilidade da proposta.
8.11. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante da demanda ou da área.
8.12. Poderão ser solicitados eventuais outros documentos complementares à proposta, que deverão ser encaminhados no prazo máximo de 02 (duas) horas.

9. DA PROVA DE CONCEITO (POC)

9.1. Definição da Prova de Conceito:

9.1.1. A prova de conceito consiste na demonstração prática dos requisitos técnicos dos módulos constantes no Termo de Referência por parte da licitante vencedora da fase de lances, do objeto que será ofertado, permitindo que seja feita a materialização da descrição do objeto ofertado pelo licitante;

9.1.2. Para que a expertise no fornecimento dos serviços a serem contratados seja considerada adequada às necessidades do CISGA, a prova de conceito será aplicada ao licitante do Pregão Eletrônico provisoriamente considerado vencedor. Atendendo às exigências definidas, o licitante será considerado apto. Não atendendo será desclassificado, sendo chamado o segundo melhor classificado para submeter-se ao mesmo processo e assim sucessivamente;

9.1.3. A avaliação apenas do vencedor provisório justifica-se pelo princípio da celeridade que rege o procedimento na modalidade pregão, conforme legislação em vigor e possui respaldo legal estabelecido na Nota Técnica n° 04/2009/TCU, bem como histórico de procedimentos similares de conhecimento público, como da Advocacia Geral da União e Supremo Tribunal Federal;

9.1.4. A prova de conceito visa permitir a averiguação das funcionalidades e características do produto sob o plano da sua real compatibilidade com o objeto licitado, não se resumindo apenas a ver no papel (mera descrição documental, abstrata).

9.2. Fases e prazos da Prova de Conceito:

9.2.1. Na fase de julgamento das propostas, será convocada a licitante provisoriamente classificada como vencedora para a realização da prova de conceito;

9.2.2. A data da sessão da prova de conceito ocorrerá 10 (dez) dias úteis após a veiculação do comunicado, divulgado no chat da plataforma de pregão eletrônico e Diário Oficial

Eletrônico do Consórcio, disponível em: https://www.cisga.com.br/portal-da-transparencia/diario-oficial-eletronico;

9.2.3. A duração da "POC" será de até dois dias, sendo que os trabalhos iniciar-se-ão às 9h e terminarão às 17h, com uma hora de intervalo para almoço a cada dia, podendo haver pequenas extensões, a critério do CISGA, caso um item esteja sob avaliação ao completar-se este horário;

9.2.4. Em caso de indisponibilidade de recursos de infraestrutura ou pessoal da Comissão Técnica, sob a responsabilidade do CISGA, que impeçam o cumprimento dos prazos definidos, haverá prorrogação pelo mesmo período de indisponibilidade.

9.3. Infraestrutura da Prova de Conceito:

9.3.1. A prova de conceito será realizada nas dependências do Consórcio, em ambiente destinado para este fim;

9.3.2. Os equipamentos, softwares base e ambiente de sistemas necessários à realização da prova de conceito são responsabilidade do licitante;

9.3.3. O Consórcio disponibilizará o espaço adequado para a apresentação dos sistemas, onde será montada uma bancada de testes, bem como disponibilizará conexão com internet de banda larga;

9.3.4. O licitante classificado provisoriamente vencedor do pregão eletrônico deve, dentro do prazo definido, preparar o ambiente para iniciar a prova de conceito;

9.3.4.1. Como o fornecedor deverá garantir o funcionamento adequado dentro do prazo definido, o CISGA, mediante agendamento prévio, pode disponibilizar acesso ao ambiente físico e equipamentos destinados à "POC" de modo que o fornecedor possa executar testes.

9.4. Custos da Prova de Conceito:

9.4.1. A prova de conceito deverá ser realizada sem custos para o Órgão Gerenciador ou Percipientes da Ate de Registro de Preços, sejam custos de serviço, pessoal, viagem, hospedagem, alimentação, investimentos em hardware e software, ou ainda qualquer outra despesa realizada pelo licitante para participar do processo licitatório e/ou da prova de conceito;

9.4.2. licitante que for reprovado na prova de conceito não terá direito a qualquer indenização;

9.4.3. A proponente será responsável pelo banco de dados de teste para a devida demonstração do sistema. Bem como deverá trazer equipamentos previamente configurados para a realização dos testes;

9.4.4. Os equipamentos poderão ser auditados pela equipe do Consórcio.

9.5. Critérios de avaliação da Prova de Conceito:

9.5.1. O CISGA nomeará uma Comissão de Apoio Técnico, que ficará responsável por realizar as avaliações, emitir relatórios e apoiar nas tomadas de decisão do Pregoeiro durante a prova de conceito;

9.5.2. É condição para a declaração da vencedora da licitação que esta efetue as comprovações de atendimento na qualidade e quantidades especificadas no Termo de Referência atingindo no mínimo 85% (oitenta e cinco por cento) dos requisitos técnicos de cada funcionalidade (módulos) relacionada no Termo de Referência;

9.5.3. O roteiro de apresentação/avaliação dos módulos seguirá a mesma ordem disposta neste termo de referência, sendo observado os requisitos técnicos relacionados a cada módulo do sistema;

9.5.4. Ao longo da demonstração, os equipamentos deverão ser operados por técnico da empresa licitante, que deverá apresentar-se na data e horário definidos pelo Consórcio Público e publicados no Diário Oficial;

9.5.5. Durante a demonstração do sistema, a Comissão de Apoio Técnico realizará a avaliação da planilha de requisitos e preencherão formulários específicos com a finalidade de comprovar o atendimento ao percentual mínimo dos requisitos técnicos de cada um dos módulos;

9.5.6. Caso o atendimento calculado, após as análises da Comissão, seja inferior ao percentual mínimo exigido, o licitante será desclassificado;

9.5.7. A fórmula utilizada para cálculo do atendimento é a seguinte:

$$Atendimento = Arredondar\ (100x\ (\frac{(Requisitos\ Atendidos)}{(Total\ de\ Requisitos)})$$

9.5.8. Atendimento é o percentual de atendimento da empresa, considerando o total de requisitos e a quantidade de requisitos atendidos pelo licitante. O percentual de atendimentos será arredondado para um número inteiro;

9.5.9. Requisitos Atendidos é a quantidade de requisitos técnicos atendidos integralmente pelo licitante de cada módulos, ratificados pela Comissão de Apoio Técnico;

9.5.10. Total Requisitos é a quantidade total de requisitos definidos para cada módulos;

9.5.11. O cálculo será feito para cada módulo que ao final da atividade, se o percentual obtido pelo licitante for menor a 85% (oitenta e cinco por cento) dos requisitos, esse será desclassificado por não atender ao mínimo exigido.

9.6. Manifestação final:

9.6.1. Comprovado o cumprimento mínimo dos requisitos, a comissão classificará a licitante mediante termo detalhado e assinado;

9.6.2. Caso a licitante melhor classificada não comprove o cumprimento mínimo dos requisitos, a comissão inabilitará a licitante e chamará, após a avaliação e aprovação dos documentos de habilitação da empresa, o próximo classificado na ordem de classificação, para respectiva demonstração de Sistema, sendo avaliada nos mesmos moldes da licitante anterior.

10. DA FASE DE HABILITAÇÃO

10.1. **Os documentos de habilitação serão solicitados pelo pregoeiro ao licitante vencedor, concedendo prazo de 02 (duas) horas para que sejam anexados no sistema, após o julgamento da proposta final**.

10.2. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia ou cópia autenticada.

10.2.1. somente haverá a necessidade de comprovação do preenchimento de requisitos mediante apresentação dos documentos originais não digitais quando houver dúvida em relação à integridade do documento digital ou quando a lei expressamente o exigir. (IN nº 3/2018, art. 4º, §1º, e art. 6º, §4º).

10.3. Na hipótese de o licitante vencedor ser empresa estrangeira que não funcione no País, para fins de assinatura do contrato ou da ata de registro de preços, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.4. Para fins de habilitação neste pregão, a licitante deverá apresentar os seguintes documentos, sob pena de inabilitação:

10.4.1. **Declarações**

a) Declaração de que atende aos requisitos de habilitação, e de que o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021);

b) Declaração de Idoneidade (de que não foi declarada inidônea por ato da Administração Pública);

c) Declaração que atende ao disposto no artigo 7°, inciso XXXIII, da Constituição Federal, nos termos do inciso VI do art. 68 da Lei nº 14.133/21;

d) Declaração que não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

e) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social;

f) Declaração da licitante de que não que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, conforme art. 14, IV da Lei nº 14.133/2021.

Declaração Exclusiva Me/Epp

a) Declaração de que cumpre os requisitos estabelecidos no artigo 3°da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos § 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021 e observância do limite de R$ 4.800.000,00 na licitação, 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. (modelo em anexo).

Declaração Exclusiva Cooperativa

b) O licitante organizado em Cooperativa deverá apresentar declaração de que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021. (modelo em anexo).

10.4.2. **Habilitação Jurídica**

a) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

c) Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

d) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

e) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

f) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

g) Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

a. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

10.4.3. **Habilitação fiscal, social e trabalhista**

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) atualizado, relativo ao domicílio ou sede do licitante, pertinente e compatível com o objeto desta licitação;

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

c) Certificado de Regularidade de Situação perante o Fundo de Garantia do Tempo de Serviço, emitido nos moldes do art. 7º, V da Lei nº 8.036, de 11 de maio de 1990;

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

e) Prova de inscrição no cadastro de contribuintes Municipal, relativo ao domicilio ou à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto Contratual;

f) Certidão de Regularidade com a Fazenda Municipal, relativa à atividade em cujo exercício contrata ou concorre, referente ao domicílio da sociedade empresária;

g) Certidão de Regularidade com a Fazenda Estadual do domicílio ou sede do licitante, dentro do prazo de validade, na forma da lei.

a. Caso o fornecedor seja considerado isento dos tributos Estaduais relacionados ao objeto contratual, ou isento da inscrição em cadastro estadual de contribuintes, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

b. o fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

10.4.4. **Qualificação Econômico-Financeira**

a) Certidão negativa de falência expedida pelo distribuidor do domicílio da sede do fornecedor, Lei nº 14.133, de 2021, art. 69, caput, inciso II).

a. Se a Certidão de falência não estabelecer prazo de validade, será considerada válida apenas a certidão com prazo de emissão não superior a 90 (noventa) dias da data da sessão.

10.4.5. **Qualificação Técnica**

a) Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;

a. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados e/ou em execução nas seguintes áreas:

i. Operação de SOC 24x7: Comprovação de fornecimento de serviço de Security Operations Center com monitoramento contínuo, detecção avançada e resposta estendida e coordenada a incidentes;

ii. Implementação e Operação de Plataforma SIEM: Experiência na implantação, tuning e operação de plataforma de correlação avançada, integrando mais de 50 fontes de dados heterogêneas;

iii. Projetos de Arquitetura Zero Trust e Controle de Acesso: Implementação de soluções de ZTNA (Zero Trust Network Access);

iv. Estratégia de Resiliência e Recuperação: Experiência em projetos de Backup Imutável e Disaster Recovery (DR);

v. Implantação e Operação Assistida da Plataforma de Maturidade em segurança da informação.

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

c. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MP n. 5, de 2017;

d. Os atestados ou declarações de capacidade técnica deverão se referir a serviços prestados no âmbito da atividade econômica principal e/ou secundária da licitante, especificada no contrato social devidamente registrado na junta comercial competente, bem como no cadastro de pessoas jurídicas da Receita Federal do Brasil – RFB;

e. Os atestados ou declarações deverão conter as seguintes informações:

i. Nome, CNPJ, dados de endereço e contato da empresa/órgão que emitiu o atestado;

ii. Nome completo e cargo do signatário;

iii. Descrição do serviço de modo a permitir a aferição de sua similaridade com o objeto licitado;

iv. Prazo de execução e quantidade contratada (se aplicável);

v. Período e local da prestação do serviço;

vi. Data de emissão do atestado;

vii. Assinatura do representante do órgão atestante.

b) Comprovação de possuir em seu quadro permanente, **na data da licitação**, ou compromisso de contratação, equipe técnica multidisciplinar com profissionais das seguintes áreas:

a. 01 Analista de sistemas;

i. Nível superior completo em áreas da Tecnologia da Informação.

b. 01 Advogado;

i. Nível superior completo em direito com registro na OAB.

c. 01 Analista de requisitos;

i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

ii. Título de especialização em engenharia de sistemas para web, gestão empresarial ou áreas afins.

d. 01 Analista de Segurança da informação;

i. Nível superior completo na área de Segurança da Informação.

e. 01 Analista de Governança Corporativa;

i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

ii. Título de especialização em governança corporativa e risco, ou áreas afins;

iii. Certificação Lead Assessor SIG ISO 37301:2021 – Gestão em Compliance – Requisitos com orientações para uso;

iv. Certificação Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019 – Gestão de Riscos e Continuidade de Negócios.

f. 01 Encarregado de Dados (DPO).

i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

ii. Certificação como Lead Assessor ISO 27001:2022 e ISO 27701:2019 – Gestão da Segurança da Informação e Gestão de Privacidade da Informação;

iii. Certificação Data Protection Officer – DPO.

1. Prova que a empresa possui vínculo com os profissionais indicados por meio de da apresentação de contrato social, em se tratando de sócio da empresa; mediante cópia da Carteira de Trabalho e Previdência Social – CTPS, no caso de empregado; por meio de contrato de prestação de serviços; ou através de declaração de contratação futura do profissional;

2. No caso de apresentação de Declaração de Contratação futura do profissional, esta deve ser acompanhada de declaração de anuência do profissional, **devidamente assinada**.

10.5. **Disposições Gerais sobre a Habilitação**

10.5.1. Quando permitida a participação de empresas estrangeiras que não funcionem no País, as exigências de habilitação serão atendidas mediante documentos equivalentes, inicialmente apresentados em tradução livre.

10.5.2. Na hipótese de o fornecedor ser empresa estrangeira que não funcione no País, para assinatura do contrato ou da ata de registro de preços ou do aceite do instrumento equivalente, os documentos exigidos para a habilitação serão traduzidos por tradutor juramentado no País e apostilados nos termos do disposto no Decreto nº 8.660, de 29 de janeiro de 2016, ou de outro que venha a substituí-lo, ou consularizados pelos respectivos consulados ou embaixadas.

10.5.3. Não serão aceitos documentos de habilitação com indicação de CNPJ/CPF diferentes, salvo aqueles legalmente permitidos.

10.5.4. Se o fornecedor for a matriz, todos os documentos deverão estar em nome da matriz, e se o fornecedor for a filial, todos os documentos deverão estar em nome da filial, exceto para atestados de capacidade técnica, e no caso daqueles documentos que, pela própria natureza, comprovadamente, forem emitidos somente em nome da matriz.

10.5.5. Serão aceitos registros de CNPJ de fornecedor matriz e filial com diferenças de números de documentos pertinentes ao CND e ao CRF/FGTS, quando for comprovada a centralização do recolhimento dessas contribuições.

10.5.6. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

10.5.7. Após a entrega dos documentos para a habilitação, não será permitida a substituição ou a apresentação de novos documentos, salvo em sede de diligência, para (Lei 14.133/21, art. 64, e IN 73/2022, art. 39, §4º):

10.5.7.1. Complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame;

10.5.7.2. Entende-se por apuração de fatos existentes à época da abertura do certame, a aferição das condições de habilitação, desde que a juntada posterior da documentação, em diligência, por solicitação e fundamentação do(a) pregoeiro(a)/agente de contratação, venha atestar condição que já existia na data da abertura da sessão pública que requereu originalmente os documentos de habilitação; (em atendimento do disciplinado no *Parecer PGE/RS 19.680/2022; Acórdão 1.211/2021-TCU-Plenário, Acórdão 2.443/2021-TCU-Plenário; Conclusão Técnica nº 27 - Comissão de Estudos da Nova Lei De Licitações e Contratos para a Fiscalização – TCE/2025*);

10.5.7.3. atualizações de documentos cuja validade tenha expirado após a data de recebimento das propostas;

10.5.7.4. suprimento da ausência de documento de cunho declaratório emitido unilateralmente pelo licitante.

10.5.8. A apresentação dos documentos de que trata o item 7.6.7 deverá ocorrer em até 2 (duas) horas do pedido de complementação de documentação realizado pelo(a) Agente de Contratação/pregoeiro(a) no chat da plataforma de pregões eletrônicos adotada.

10.5.9. Findo o prazo assinalado sem o envio da nova documentação, restará decadente essa oportunidade conferida ao licitante, implicando sua inabilitação.

10.5.10. Nos termos dos artigos 42 e 43 da Lei Complementar nº 123/06, as Microempresas e Empresas de Pequeno Porte deverão apresentar toda a documentação exigida para a habilitação, mesmo que esta apresente alguma restrição com relação à regularidade fiscal e trabalhista.

10.5.11. Havendo alguma restrição na comprovação da regularidade fiscal e trabalhista, será assegurado o prazo de 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 pública, para regularização da documentação, para pagamento ou parcelamento do débito e para emissão de eventuais certidões negativas ou positivas com efeito de certidão negativa.

10.5.12. A não regularização da documentação no prazo previsto acima implicará decadência do direito de contratação, sem prejuízo das sanções previstas no art. 90 da Lei Federal nº 14.133/21, sendo facultado à Administração convocar os licitantes remanescentes, na ordem de classificação, para contratação, ou revogar a licitação.

10.5.13. Na análise dos documentos de habilitação, o pregoeiro poderá sanar erros ou falhas, que não alterem a substância dos documentos e sua validade jurídica, mediante decisão

fundamentada, registrada em ata e acessível a todos, atribuindo-lhes eficácia para fins de habilitação e classificação.

10.5.14. Na hipótese de o licitante não atender às exigências para habilitação, o pregoeiro examinará a proposta subsequente e assim sucessivamente, na ordem de classificação, até a apuração de uma proposta que atenda ao presente edital, observado o prazo disposto no subitem 9.1.

10.5.15. Somente serão disponibilizados para acesso público os documentos de habilitação do licitante cuja proposta atenda ao edital de licitação, após concluídos os procedimentos de que trata o subitem anterior.

11. DA ATA DE REGISTRO DE PREÇOS

11.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 5 (cinco) dias, contados a partir da data de sua convocação, para assinar a Ata de Registro de Preços, cujo prazo de validade encontra-se nela fixado, sob pena de decadência do direito à contratação, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

11.2. O prazo de convocação poderá ser prorrogado uma vez, por igual período, mediante solicitação do licitante mais bem classificado ou do fornecedor convocado, desde que:

11.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e

11.2.2. a justificativa apresentada seja aceita pela Administração.

11.3. **A Ata de Registro de Preços deverá ser assinada por meio de assinatura digital Qualificada ICP-Brasil, através do acesso ao Sistema de Controle de Licitações e Contratos Administrativos CLIC – CISGA**.

11.4. Serão formalizadas tantas Atas de Registro de Preços quantas forem necessárias para o registro de todos os itens constantes no Termo de Referência, com a indicação do licitante vencedor, a descrição do(s) item(ns), as respectivas quantidades, preços registrados e demais condições.

11.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da Ata de Registro de Preços.

11.6. A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a contratação pretendida, desde que devidamente justificada.

11.7. Na hipótese de o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidas, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

11.8. O prazo de vigência da ata de registro de preços será de 1 (um) ano e poderá ser prorrogado, por igual período, desde que comprovado o preço vantajoso.

11.9. Em caso de prorrogação da ata, poderá ser renovado o quantitativo originalmente registrado.

12. DA FORMAÇÃO DO CADASTRO DE RESERVA

12.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:

12.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e

12.1.2. dos licitantes que mantiverem sua proposta original.

12.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.

12.3. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.
12.4. Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem cotar o objeto com preço igual ao do adjudicatário antecederão aqueles que mantiverem sua proposta original.
12.5. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

12.5.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou

12.5.2. quando houver o cancelamento do registro do fornecedor ou do registro de preços, nas hipóteses previstas nos art. 28 e art. 29 do Decreto nº 11.462/23.

12.6. Na hipótese de nenhum dos licitantes que aceitaram cotar o objeto com preço igual ao do adjudicatário concordar com a contratação nos termos em igual prazo e nas condições propostas pelo primeiro classificado, a Administração, observados o valor estimado e a sua eventual atualização na forma prevista no edital, poderá:

12.6.1. convocar os licitantes que mantiveram sua proposta original para negociação, na ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

12.6.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

13. DO TERMO DE CONTRATO

13.1. Após a homologação e adjudicação e assinatura da Ata de Registro de Preços, caso se conclua pela contratação, será firmado termo de contrato com o CISGA, ou outro instrumento equivalente.
13.2. O adjudicatário terá o prazo de 5 dias úteis, contados a partir da data de sua convocação, para assinar o termo de contrato sob pena de decair o direito à contratação, sem prejuízo das sanções previstas neste Edital.

13.2.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura do Termo de Contrato ou instrumento equivalente, a Administração poderá:

13.2.1.1. encaminhá-lo para assinatura, mediante correspondência postal com aviso de recebimento (AR), para que seja assinado e devolvido no prazo de 5 dias úteis, a contar da data de seu recebimento;

13.2.1.2. disponibilizar acesso a sistema de processo eletrônico para que seja assinado digitalmente em até 5 dias úteis; ou

13.2.1.3. outro meio eletrônico, assegurado o prazo de 5 dias úteis para resposta após recebimento da notificação pela Administração.

13.3. O prazo do item 13.2 poderá ser prorrogado, por igual período, por solicitação justificada do adjudicatário e aceite pela Administração.
13.4. O prazo de vigência da contratação é o estabelecido no Termo de Referência.

14. DOS RECURSOS

14.1. A interposição de recurso referente ao julgamento das propostas, à habilitação ou inabilitação de licitantes, à anulação ou revogação da licitação, observará o disposto no art. 165 da Lei nº 14.133, de 2021.

14.2. O prazo recursal é de 3 (três) dias úteis, contados da data de intimação.
14.3. Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:
14.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;
14.3.2. o prazo para a manifestação da intenção de recorrer será de 10 (dez) minutos;
14.3.3. o prazo para apresentação das razões recursais será iniciado na data de intimação;
14.3.4. os recursos deverão ser encaminhados em campo próprio do sistema.
14.4. O recurso será dirigido à autoridade que tiver editado o ato ou proferido a decisão recorrida, a qual poderá reconsiderar sua decisão no prazo de 3 (três) dias úteis, ou, nesse mesmo prazo, encaminhar recurso para a autoridade superior, a qual deverá proferir sua decisão no prazo de 10 (dez) dias úteis, contado do recebimento dos autos.
14.5. Os recursos interpostos fora do prazo não serão conhecidos.
14.6. O prazo para apresentação de contrarrazões ao recurso pelos demais licitantes será de 3 (três) dias úteis, contados da data da intimação pessoal ou da divulgação da interposição do recurso, assegurada a vista imediata dos elementos indispensáveis à defesa de seus interesses.
14.7. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
14.8. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
14.9. Os autos do processo permanecerão com vista franqueada aos interessados no sítio eletrônico https://www.cisga.com.br/licitacoes.

15. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

15.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:
15.1.1. deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pelo/a pregoeiro/a durante o certame;
15.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta em especial quando:
15.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;
15.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;
15.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou
15.1.2.4. deixar de apresentar amostra;
15.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;
15.1.2.6. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
15.1.2.7. recusar-se, sem justificativa, a assinar o contrato ou a ata de registro de preço, ou a aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração;
15.1.2.8. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;
15.1.2.9. fraudar a licitação;
15.1.2.10. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
15.1.2.10.1. agir em conluio ou em desconformidade com a lei;
15.1.2.10.2. induzir deliberadamente a erro no julgamento;
15.1.2.10.3. apresentar amostra falsificada ou deteriorada;
15.1.2.10.4. praticar atos ilícitos com vistas a frustrar os objetivos da licitação;
15.1.2.10.5. praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013.

15.2. Com fulcro na Lei nº 14.133, de 2021, a Administração poderá, após regular processo administrativo, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:

15.2.1. advertência;

15.2.2. multa;

15.2.3. impedimento de licitar e contratar; e

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

15.3. Na aplicação das sanções serão considerados:

15.3.1. a natureza e a gravidade da infração cometida;

15.3.2. as peculiaridades do caso concreto;

15.3.3. as circunstâncias agravantes ou atenuantes;

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

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

15.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **15 (quinze) dias úteis**, a contar da comunicação oficial.

15.5. Para as infrações previstas nos itens 15.1.1, 15.1.2, 15.1.2.1, 15.1.2.2, 15.1.2.3, 15.1.2.4, 15.1.2.5, 15.1.2.6, 15.1.2.7 a multa será de 0,5% a 15% do valor do contrato licitado.

15.6. Para as infrações previstas nos itens 15.1.2.8, 15.1.2.9, 15.1.2.10, 15.1.2.10.1, 15.1.2.10.2, 15.1.2.10.3, 15.1.2.10.4, 15.1.2.10.5 a multa será de 15% a 30% do valor do contrato licitado.

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

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

15.9. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 15.1.1, 15.1.2, 15.1.2.1, 15.1.2.2, 15.1.2.3, 15.1.2.4, 15.1.2.5, 15.1.2.6, 15.1.2.7, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar no âmbito da Administração Pública direta e indireta do ente federativo a qual pertencer o órgão ou entidade, pelo prazo máximo de 3 (três) anos.

15.10. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 15.1.2.8, 15.1.2.9, 15.1.2.10, 15.1.2.10.1, 15.1.2.10.2, 15.1.2.10.3, 15.1.2.10.4, 15.1.2.10.5, bem como pelas infrações administrativas previstas nos itens 15.1.1, 15.1.2, 15.1.2.1, 15.1.2.2, 15.1.2.3, 15.1.2.4, 15.1.2.5, 15.1.2.6, 15.1.2.7 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar, cuja duração observará o prazo previsto no art. 156, §5º, da Lei n.º 14.133/2021.

15.11. A recusa injustificada do adjudicatário em assinar o contrato ou a ata de registro de preço, ou em aceitar ou retirar o instrumento equivalente no prazo estabelecido pela Administração, descrita no item 15.1.2.6, caracterizará o descumprimento total da obrigação assumida e o sujeitará às penalidades e à imediata perda da garantia de proposta em favor do órgão ou entidade promotora da licitação, nos termos do art. 45, §4º da IN SEGES/ME n.º 73, de 2022.

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

15.13. Caberá recurso no prazo de 15 (quinze) dias úteis da aplicação das sanções de advertência, multa e impedimento de licitar e contratar, contado da data da intimação, o qual será dirigido à autoridade que tiver

proferido a decisão recorrida, que, se não a reconsiderar no prazo de 5 (cinco) dias úteis, encaminhará o recurso com sua motivação à autoridade superior, que deverá proferir sua decisão no prazo máximo de 20 (vinte) dias úteis, contado do recebimento dos autos.

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

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

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

15.17. Para a garantia da ampla defesa e contraditório dos licitantes, as notificações serão enviadas eletronicamente para os endereços de e-mail informados na proposta comercial.

15.17.1. Os endereços de e-mail informados na proposta comercial serão considerados de uso contínuo da empresa, não cabendo alegação de desconhecimento das comunicações a eles comprovadamente enviadas.

16. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

16.1. Qualquer pessoa é parte legítima para impugnar este Edital por irregularidade na aplicação da Lei nº 14.133, de 2021, devendo protocolar o pedido até 3 (três) dias úteis antes da data da abertura do certame.

16.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgado em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.

16.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, pelo seguinte meio, e-mail: contato@cisga.com.br

16.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.

16.5. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.

16.6. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

17. DA ADEQUAÇÃO ORÇAMENTÁRIA

17.1. As despesas correrão por conta de dotação específica dos orçamentos de cada CONTRATANTE, sendo que no momento da contratação será especificada a dotação orçamentária.

17.2. O Ente CONTRATANTE quando da contratação especificará a classificação orçamentária.

18. DAS DISPOSIÇÕES GERAIS

18.1. Será divulgada ata da sessão pública no sistema eletrônico:

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

18.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília – DF.

18.4. A homologação do resultado desta licitação não implicará direito à contratação.

18.5. As normas disciplinadoras da licitação serão sempre interpretadas em favor da ampliação da disputa entre os interessados, desde que não comprometam o interesse da Administração, o princípio da isonomia, a finalidade e a segurança da contratação.

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

18.7. Na contagem dos prazos estabelecidos neste Edital e seus Anexos, excluir-se-á o dia do início e incluir-se-á o do vencimento. Só se iniciam e vencem os prazos em dias de expediente na Administração.

18.8. O desatendimento de exigências formais não essenciais não importará o afastamento do licitante, desde que seja possível o aproveitamento do ato, observados os princípios da isonomia e do interesse público.

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

18.10. Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico https://www.cisga.com.br/licitacoes, além de disponível no https://pregaobanrisul.com.br/.

19. DOS DOCUMENTOS INTEGRANTES AO EDITAL

19.1. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:

19.1.1. Anexo I - Termo de Referência;
19.1.2. Anexo II - Modelo de Proposta de Preços;
19.1.3. Anexo III - Minuta de Ata de Registro de Preços;
19.1.4. Anexo IV - Minuta do Contrato de Fornecimento;
19.1.5. Anexo V - Declarações – Habilitação (modelo);
19.1.6. Anexo VI - Declaração Exclusiva ME/EPP (modelo);
19.1.7. Anexo VII- Declaração Exclusiva Cooperativa (modelo);
19.1.8. Anexo VIII - Declaração de Identificação dos Profissionais Envolvidos na Prestação de Serviços (modelo);
19.1.9. Anexo IX - Catálogo Técnico de Unidade de Serviço Técnico (UST);
19.1.10. Anexo X - Estudo Técnico Preliminar.

Garibaldi, 24 de setembro de 2026.

RUDIMAR CABERLON:47751517034
Assinado de forma digital por RUDIMAR CABERLON:47751517034
Dados: 2026.09.24 08:30:06 -03'00'

RUDIMAR CABERLON
Diretor Executivo CISGA

NELTON CARLOS CONTE:53096797072
Assinado de forma digital por NELTON CARLOS CONTE:53096797072
Dados: 2026.09.24 13:13:43 -03'00'

NELTON CARLOS CONTE
Presidente Consórcio Intermunicipal de Desenvolvimento Sustentável da Serra Gaúcha CISGA

TERMO DE REFERÊNCIA

Processo Administrativo n° 031/2026

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA, conforme especificações e condições estabelecidas no Termo de Referência e seus anexos;

1.2. Das quantidades a serem contratadas:

Item	**Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, compreendendo serviço de adequação à LGPD e manutenção recorrente, firewalls de próxima geração (NGFW), gerenciamento centralizado e retenção de logs, serviço gerenciado de monitoramento e resposta a incidentes (NOC/SOC/SIEM), software de antivírus com VPN/ZTNA, backup em nuvem, transceivers, treinamento e horas técnicas de suporte especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA.**	Unidade	Quantidade
01	Implantação do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I, II, III.	UST (unidade)	20.208
02	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I	Até 30.00 Habitantes (mês)	192
03	Terceirização do Encarregado de Dados – Tipo I	Até 30.000 Habitantes (mês)	192
04	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo II	De 30.001 até 50.000 habitantes (mês)	36
05	Terceirização do Encarregado de Dados – Tipo II	De 30.001 até 50.000 habitantes (mês)	36
06	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo III	De 50.001 até 100.000 habitantes (mês)	12
07	Terceirização do Encarregado de Dados – Tipo III	De 50.001 até 100.000 habitantes	12

		(mês)	
08	Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
09	Operação Assistida e Treinamento para Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente.	UST (unidade)	7.680
10	Solução de Detecção e Resposta a Incidentes em Endpoints (EDR) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
11	Operação Assistida e Treinamento para Solução de Detecção e Resposta a Incidentes em Endpoints (EDR)	UST (unidade)	7.680
12	Solução de Proteção e Prevenção de Vazamento de Dados (DLP) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
13	Operação Assistida e Treinamento para Solução de Proteção e Prevenção de Vazamento de Dados (DLP).	Endpoint (unidade)	7.680
14	Software de SIEM - Security Information&Event Managment com setup/implantação e suporte de 12 meses.	Ativo Monito-rado (unidade)	3.552
15	Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos, conformidade, maturidade com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
16	Operação Assistida e Treinamento para Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos, conformidade, maturidade.	UST (unidade)	7.680
17	Sistema de Backup Resilente, recuperação via DR Online com setup/implantação e suporte de 12 meses.	TB Protegido (unidade)	2.604
18	Operação Assistida e Treinamento para Sistema de Backup Resilente, recuperação via DR Online.	UST (unidade)	7.680
19	SOC - Security Operations Center – 8x5 com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	39.192

20	SOC - Security Operations Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	33.288
21	Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM), com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
22	Operação Assistida e Treinamento para Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM).	UST (unidade)	7.680
23	Contratação de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados de ransomware com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
24	Operação Assistida e Treinamento para Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados.	UST (unidade)	7.680
25	Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
26	Operação Assistida e Treinamento para Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação.	UST (unidade)	7.680
27	NOC – Network Operation Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	3.552
28	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo I com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	5
29	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo II com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	12
30	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo III com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	6
31	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo IV com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	5
32	Subscrição anual de plataforma em nuvem de criptografia, anonimização e rastreabilidade documental.	Subscrição anual por muni-cípio/Orgao (mês)	240
33	Crédito de anonimização excedente à franquia	Mil páginas equivalentes (unidade)	303
34	Crédito de custódia cifrada excedente à franquia	Mil arquivos (unidade)	125
35	Crédito de armazenamento excedente à franquia	Gigabyte (unidade)	1.485

36	Crédito de rastreabilidade excedente à franquia	Mil Páginas Marcadas (unidade)	157
37	Operação Assistida e Treinamento para itens – 33 ao 36	UST (unidade)	7.680

1.3. A presente licitação ocorrerá pelo Sistema de Registro de Preços, nos termos dos artigos 82 a 86 da Lei n.º 14.133/2021 e do Decreto Federal º 11.462/2023, de acordo o disposto neste Termo de Referência;

1.4. O Sistema de Registro de Preços encontra-se amparado pela(s) hipótese(s) abaixo (conforme art. 3º, Decreto Federal nº 11.462, de 31 de março de 2023):

1.4.1. há necessidade de contratações permanentes ou frequentes em razão das características do objeto;

1.4.2. é conveniente a aquisição de bens com previsão de entregas parceladas;

1.4.3. não é possível definir previamente o quantitativo a ser demandado em razão da natureza do objeto;

1.4.4. por se tratar de licitação compartilhadas, é conveniente para atendimento a mais de um órgão ou a mais de uma entidade.

1.5. A validade da Ata de Registro de Preços será de 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso;

1.5.1. O contrato decorrente da Ata de Registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro;

1.5.2. Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

1.6. A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021;

1.6.1. O instrumento contratual de que trata o item 1.6 deverá ser assinado no prazo de validade da ata de registro de preços.

1.7. O prazo de vigência da contratação é de 12 (doze) meses, contados a partir do primeiro dia útil subsequente à data de divulgação no PNCP;

1.8. Tratando-se de contratação que prevê operação continuada do sistema, prazo de vigência da contratação é de 12 (doze) meses, prorrogável para até 10 anos (máximo de 10 anos, incluindo prorrogações), contados do(a) a partir do primeiro dia útil subsequente à data de divulgação no PNCP na forma do artigo 107 da Lei n° 14.133, de 2021;

1.9. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data limite para a apresentação das propostas;

1.10. Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Indice de Custo da Tecnologia da Informação (ICTI), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula:

1.10.1. $V_R = V_O \text{ X } \left(\frac{If}{Il}\right)$, onde =

1.10.1.1. V_R = **Valor reajustado** (novo preço do contrato);

1.10.1.2. V_O = **Valor original** do contrato ou parcela a ser reajustada;

1.10.1.3. I_F = **Índice final**, correspondente ao número-índice do mês de corte do reajuste;

1.10.1.4. I_I = **Índice inicial**, correspondente ao número-índice da data-base (ex: data do orçamento estimado).

1.11. Caso o índice de reajuste (ICTI) apresente variação negativa ou zero, o valor do contrato será mantido inalterado até o próximo período de reajuste;

1.11.1. O contratante será notificado do valor atualizado por escrito, com antecedência mínima de 15 (quinze) dias antes da data do reajuste.

1.12. O contrato oferecerá maior detalhamento das regras que serão aplicadas em relação à vigência da contratação.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

2.1. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

3. DA CLASSIFICAÇÃO E DA CONTINUIDADE DO SERVIÇO

3.1. O serviço objeto desta contratação são caracterizados como comuns, conforme justificativa constante do Estudo Técnico Preliminar;

3.2. O serviço é enquadrado como continuado, tendo em vista que tem como objetivo atender à necessidade pública de forma permanente e contínua, conforme justificativa constante do Estudo Técnico Preliminar.

4. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

4.1. A fundamentação e descrição da necessidade da contratação encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

5. REQUISITOS DE GARANTIA E MANUTENÇÃO

5.1. O prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), e suas atualizações.

6. REQUISITOS DE METODOLOGIA DE TRABALHO

6.1. A execução dos serviços está condicionada a assinatura do contrato e ao recebimento pelo Contratado de Ordem de Serviço (OS) ou Autorização de Fornecimento emitida pela Contratante;

6.2. A OS ou Autorização de Fornecimento indicará o serviço, a quantidade e a localidade na qual os deverão ser prestados;

6.3. A execução do serviço dever ser acompanhada pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.

7. SUSTENTABILIDADE

7.1. Os critérios de sustentabilidade encontram-se pormenorizados no tópico Sustentabilidade do Estudo Técnico Preliminar, apêndice deste Termo de Referência.

8. SUBCONTRATAÇÃO

8.1. É vedada a subcontratação ou transferência total ou parcial do objeto da licitação, conforme justificativa pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

9. GARANTIA DA CONTRATAÇÃO

9.1. Não haverá exigência da garantia da contratação dos artigos 96 e seguintes da Lei nº 14.133, de 2021, pelas razões constantes do Estudo Técnico Preliminar.

10. LOCAL E HORÁRIO DA PRESTAÇÃO DOS SERVIÇOS QUANDO PRESENCIAIS

10.1. Os serviços objeto da presente contratação serão executados, predominantemente, em ambiente virtual, por meio de plataforma eletrônica e demais ferramentas tecnológicas disponibilizadas pela contratada.

10.2. Excepcionalmente, quando a natureza da atividade exigir a presença física, como na realização de treinamentos, reuniões técnicas ou outras ações previamente justificadas, os serviços poderão ser prestados de forma presencial na sede do CONTRATANTE, sem prejuízo das demais condições estabelecidas no instrumento convocatório.

11. MECANISMOS FORMAIS DE COMUNICAÇÃO

11.1. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:

11.1.1. Ordem de Serviço/Autorização de Fornecimento;

11.1.2. Ata de Reunião;

11.1.3. Ofício;

11.1.4. Sistema de abertura de chamados;

11.1.5. E-mails;

11.1.6. Cartas;

11.1.7. Entre outros meios.

12. PREPOSTO

12.1. A Contratada designará formalmente o preposto da empresa, antes do início da prestação dos serviços, indicando no instrumento os poderes e deveres em relação à execução do objeto contratado;

12.2. Contratante poderá recusar, desde que justificadamente, a indicação ou a manutenção do preposto da empresa, hipótese em que a Contratada designará outro para o exercício da atividade.

13. REUNIÃO INICIAL

13.1. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, poderá será realizada a Reunião Inicial de alinhamento com o objetivo de nivelar os entendimentos acerca das condições estabelecidas no Contrato, Edital e seus anexos, e esclarecer possíveis dúvidas acerca da execução dos serviços.

13.2. A reunião será realizada em conformidade com o previsto no inciso I do Art. 31 da IN SGD/ME nº 94, de 2022, e ocorrerá em data a ser convencionada entre as partes.

13.3. Nas reuniões de início deverão obrigatoriamente ser tratados os temas:

13.3.1. A LGPD e seus aspectos direcionados à Administração Pública;

13.3.2. A importância da conformidade para a CONTRATANTE;

13.3.3. O projeto de adequação;

13.3.4. O processo de construção do programa de conformidade com a LGPD;

13.3.5. A definição dos agentes envolvidos e seus respectivos papéis de acordo com a Lei Geral de Proteção de Dados;

13.3.6. A pauta desta reunião observará, pelo menos:

13.3.6.1. Presença do representante legal da contratada, que apresentará o seu preposto;

13.3.6.2. A Carta de apresentação do Preposto deverá conter no mínimo o nome completo e CPF do funcionário da empresa designado para acompanhar a execução do contrato e atuar como interlocutor principal junto à Contratante, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual;

13.3.6.3. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;

13.3.6.4. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;

13.3.6.5. O repasse à contratada de conhecimentos necessários à execução dos serviços;

13.4. A disponibilização de infraestrutura à contratada para demonstrações e analise, quando couber.

14. DO ESCOPO DOS SERVIÇOS E ESPECIFICAÇÕES TÉCNICAS

Software de adequação e manutenção da LGPD

14.1. Os serviços disponíveis no software de adequação à LGPD, contemplados nesta contratação, serão agrupados em fases de acordo com as suas finalidades e afinidades, adiante especificadas, podendo a

CONTRATANTE alterar a ordem de realização destas, se possível, e de acordo com a necessidade e com o intuito de melhorar o resultado esperado:

14.1.1. Implantação do software de adequação;

14.1.2. Disponibilização de modulo de atendimento das requisições dos titulares;

14.1.3. Treinamento da equipe de implementação;

14.1.4. Treinamento e conscientização dos empregados;

14.1.5. Identificação dos processos;

14.1.6. Inventário de dados;

14.1.7. Gestão dos Riscos;

14.1.8. Controles Internos;

14.1.9. Planos de Ação para implementação dos controles;

14.1.10. Definição da Política de Privacidade;

14.1.11. Definição dos termos de consentimento;

14.1.12. Geração dos Relatórios de Impacto à Proteção de Dados.

Da implantação do software de adquação

14.2. O software deverá rodar em nuvem e ficar hospedado no ambiente da CONTRATADA;

14.3. O software deverá possuir licenças específicas para usuários e administradores, sendo disponibilizadas o número de licenças limitado ao porte de cada município/contratante, suficientes para uso do município/contratante em cada secretaria;

14.4. O software deverá possuir controle de acessos, com níveis diferenciados para administrador e operador;

14.5. Deverá ser ministrado curso para a utilização de todos os componentes do Software, logo que implantado.

Funcionalidades do Software

14.6. O software deverá ser composto por módulos que deverão ser guiados por formulários de preenchimento com os requisitos necessários ao atendimento da LGPD, devendo também manter armazenados em banco de dados relacional todos os dados preenchidos.

14.7. Consiste no desenvolvimento e configuração dos dódulos da Plataforma:

14.7.1. **Módulo 1 - Administração – este módulo deverá**:

14.7.1.1. Permitir a definição dos parâmetros essenciais para o funcionamento do sistema, incluindo configurações de e-mail (SMTP, porta, usuário, senha, remetente) e de domínio (URL, IP e demais dados obrigatórios);

14.7.1.2. Garantir que tais parâmetros assegurem o correto envio de notificações internas e externas, bem como a integração entre os módulos;

14.7.1.3. Possibilitar a alteração e atualização dessas informações pelo administrador do sistema a qualquer momento, com registro das modificações realizadas;

14.7.1.4. Possibilitar o cadastro de múltiplas empresas dentro da plataforma, com identificação por CNPJ, nome da organização e status (ativo/inativo);

14.7.1.5. Permitir a vinculação das empresas cadastradas a processos, áreas, contratos, riscos e demais funcionalidades do sistema;

14.7.1.6. Garantir a integridade e a rastreabilidade das informações organizacionais, de modo que somente administradores autorizados possam alterar dados cadastrais;

14.7.1.7. Permitir o cadastro das áreas da organização;

14.7.1.8. Permitir visualizar as áreas e formato de organograma;

14.7.1.9. Permitir o cadastro de usuários com dados como nome completo, e-mail, cargo e perfil de acesso;

14.7.1.10. Possibilitar a definição de permissões personalizadas por perfil, garantindo segregação de funções e segurança da informação;

14.7.1.11. Garantir que os usuários recebam credenciais de acesso de forma segura, com envio automático de instruções para criação ou recuperação de senha;

14.7.1.12. Possibilitar a inativação de usuários sem exclusão de seu histórico de atividades, preservando rastreabilidade;

14.7.1.13. Assegurar que o controle de acesso possa ser configurado por categoria de informação ou por item individual (ex.: documento ou processo específico);

14.7.1.14. Possibilitar a geração de relatórios sobre empresas e usuários cadastrados, incluindo status, perfis e alterações realizadas;

14.7.1.15. Garantir trilha de auditoria completa das ações administrativas (cadastros, edições, inativações, permissões), assegurando conformidade e transparência.

14.7.2. **Módulo 2 - Processos – este módulo deverá**:

14.7.2.1. Permitir o registro de processos organizacionais, com, no mínimo, campos para título, descrição, responsável, área relacionada e situação;

14.7.2.2. Possibilitar a inclusão de informações complementares, como documentos de apoio, anexos e observações;

14.7.2.3. Garantir a vinculação dos processos às áreas, sistemas e fornecedores previamente cadastrados no módulo de Domínio;

14.7.2.4. Disponibilizar editor gráfico para desenho de fluxogramas de processos em notação BPMN, dentro da própria ferramenta;

14.7.2.5. Permitir salvar, editar e atualizar o fluxograma diretamente na ferramenta, com preservação de histórico de alterações;

14.7.2.6. Possibilitar a exportação e importação dos fluxogramas para formatos padrão, assegurando interoperabilidade e backup;

14.7.2.7. Permitir o versionamento dos processos;

14.7.2.8. Permitir que os processos sejam revisados e atualizados a qualquer momento mediante justificativa;

14.7.2.9. Garantir que alterações significativas tramitem em fluxo de aprovação antes de publicação;

14.7.2.10. Possibilitar a preservação de histórico completo de versões, identificando autor, data e justificativa da alteração;

14.7.2.11. Possibilitar a associação dos processos com o Inventário de Dados, de modo que as atividades cadastradas sejam vinculadas ao tratamento de dados pessoais;

14.7.2.12. Permitir integração com o Módulo de Riscos, possibilitando vinculação de riscos aos processos mapeados;

14.7.2.13. Permitir integração com o Módulo de Planos de Ação, vinculando ações mitigadoras ou corretivas aos processos correspondentes;

14.7.2.14. Garantir que o acesso aos processos cadastrados seja controlado por perfis de usuário, podendo ser configurado por categoria de processo ou individualmente por processo;

14.7.2.15. Assegurar que somente usuários autorizados possam visualizar, editar ou aprovar processos, conforme as permissões atribuídas;

14.7.2.16. Possibilitar a geração de relatórios dos processos cadastrados, incluindo status, responsáveis, fluxogramas e vínculos com dados, riscos e controles;

14.7.2.17. Permitir exportação dos relatórios em formatos XLS e PDF;

14.7.2.18. Manter trilha de auditoria completa, com registro de todas as inclusões, alterações, aprovações e exclusões.

14.7.3. **Módulo 3 - Inventário – este módulo deverá**:

14.7.3.1. Registrar o Registro de Operações de Tratamento de Dados (ROPA) como inventário oficial das operações de tratamento de dados da organização;

14.7.3.2. Exigir a associação de cada registro de ROPA a um Processo previamente cadastrado no Módulo de Processos;

14.7.3.3. Possuir campos que permitam cadastrar os dados que são coletados e tratados nos processos cadastrados;

14.7.3.4. Possuir campos que permitam cadastrar a finalidade de uso destes dados;

14.7.3.5. Possuir campos que permitam cadastrar como os dados são coletados e o local da coleta;

14.7.3.6. Possuir campos que permitam cadastrar como os dados são armazenados e recuperados;

14.7.3.7. Possuir campos que permitam cadastrar se os dados são compartilhados, com quem e como é feito este compartilhamento;

14.7.3.8. Possuir campos que permitam cadastrar a forma como é feito o descarte dos dados;

14.7.3.9. Possuir campos que permitam cadastrar quais são as bases legais para garantir a legalidade no tratamento de dados;

14.7.3.10. Possuir campos que permitam cadastrar como se dá o término do tratamento;

14.7.3.11. Possibilitar submeter novos registros e revisões do ROPA a fluxo de aprovação com notificações aos aprovadores.

14.7.4. **Módulo 4 - Gestão de Riscos – este módulo deverá:**

14.7.4.1. Permitir que seja feito todo o gerenciamento de riscos que envolvam incidentes com dados pessoais:

14.7.4.2. Possuir dicionário de riscos cadastrado previamente na ferramenta, possibilitando que o operador associe riscos pré-cadastrados aos processos, previamente cadastrados, em análise;

14.7.4.3. Permitir a inclusão de novos riscos que não estejam no dicionário nativo;

14.7.4.4. Permitir a avaliação dos riscos, possibilitando a escolha do método (Os métodos são nativos da ferramenta);

14.7.4.5. Permitir a priorização dos riscos por severidade;

14.7.4.6. Possuir dicionário de controles internos cadastrado previamente na ferramenta;

14.7.4.7. Permitir a inclusão de novos controles internos que não estejam no dicionário nativo;

14.7.4.8. Permitir a associação dos controles internos aos riscos já associados/cadastrados.

14.7.5. **Módulo 5 - Plano de Ação – este módulo deverá.**

14.7.5.1. Permitir o cadastro e acompanhamento dos planos de ação, no modelo 5W2H, para garantir a efetividade das implantações dos controles internos que ainda não estão em uso na organização;

14.7.5.2. Permitir a criação de planos de ação novos;

14.7.5.3. Permitir associar um plano de ação a um controle ainda não implantado;

14.7.5.4. Permitir que sejam instanciados usuários responsáveis pelas ações planejadas;

14.7.5.5. Permitir o acompanhamento da execução dos planos de ação;

14.7.5.6. Permitir a reprogramação das ações e dos planos;

14.7.5.7. Permitir a geração de relatórios dos planos de ação.

14.7.6. **Módulo 6 - Avisos Legais – este módulo deverá**:

14.7.6.1. Permitir a geração automática, com base na escolha do usuário e algumas seleções de informações necessárias, os avisos legais necessários para garantir a conformidade da organização à LGPD;

14.7.6.2. Possuir os avisos legais pré configurados e gerados automaticamente;

14.7.6.3. Possibilitar que os dados cadastrados nos demais módulos sejam carregados para os avisos legais, sem necessidade de digitação do operador ou de comandos de área de transferência (copiar e colar);

14.7.6.4. Possibilitar a geração automática do RIPD – Relatório de Impacto à Proteção de Dados Pessoais (art. 5º, inciso V - art. 32 – art. 38);

14.7.6.5. Possibilitar a geração automática da Política de Proteção e Privacidade de Dados Pessoais (art. 50, inciso I-a);

14.7.6.6. Possibilitar a geração automática de Termos de consentimento;

14.7.6.7. Possibilitar a geração automática do Termo de uso de cookies;

14.7.6.8. Possibilitar editar qualquer um dos documentos listados, dentro da própria ferramenta.

14.7.7. **Módulo 7 - DSR – este módulo deverá**:

14.7.7.1. Permitir que sejam gerenciadas e atendidas as requisições dos titulares de dados, também chamadas de DSR - Data Subject Request ou Solicitação do Titular dos Dados em português, para atendimento do Art. 18 da LGPD;

14.7.7.2. Disponibilizar formulário web para abertura da requisição, a ser incorporado no site do controlador ou operador de dados;

14.7.7.3. Possibilitar a validação da titularidade do requisitante, de forma automatizada;

14.7.7.4. Possibilitar a visualização e gestão das requisições que entram via formulário;

14.7.7.5. Permitir a seleção de uma requisição especifica, entrando nos detalhes da mesma;

14.7.7.6. Permitir que as requisições sejam respondidas por dentro da própria ferramenta;

14.7.7.7. Possibilitar o acompanhamento dos prazos das interações;

14.7.7.8. Possibilitar que todas as interações, seja do DPO ou do titular, sejam feitas por dentro da ferramenta;

14.7.7.9. Permitir a geração de relatórios das requisições.

14.7.8. **Módulo 8 - Gestão de Contratos – este módulo deverá**:

14.7.8.1. Possibilitar o cadastro de todos os contratos da organização;

14.7.8.2. Possibilitar anexar os arquivos dos contratos;

14.7.8.3. Notificar o responsável quando o contrato estiver próximo do vencimento e na data em que estiver vencendo;

14.7.8.4. Permitir identificar a severidade dos contratos, com base em perguntas predefinidas e pesos das respostas, a serem definidos;

14.7.8.5. Possibilitar a geração de relatórios dos contratos;

14.7.8.6. Permitir a visualização de contratos através de filtros estabelecidos;

14.7.8.7. Possibilitar um fluxo de aprovação no contrato, que gere tarefas ao aprovador.

14.7.9. **Módulo 9 - Gestão de Cookies – este módulo deverá**:

14.7.9.1. Possibilitar a configuração de banner de cookies customizável para exibição no site da contratante;

14.7.9.2. Permitir a categorização dos cookies em: estritamente necessários, de desempenho, de funcionalidade e de publicidade/marketing;

14.7.9.3. Permitir que o titular aceite ou rejeite os cookies por categoria;

14.7.9.4. Possibilitar a revisão ou alteração do consentimento pelo titular a qualquer momento;

14.7.9.5. Armazenar o registro do consentimento dado pelo titular, incluindo data, hora, localização, versão da política de cookies e preferências selecionadas;

14.7.9.6. Permitir exportar o histórico de consentimentos em relatórios, para fins de auditoria;

14.7.9.7. Possibilitar a varredura automática do site para identificar cookies em uso, informando sua origem, finalidade, duração e categoria;

14.7.9.8. Permitir o cadastro manual de cookies não detectados automaticamente;

14.7.9.9. Possibilitar a atualização periódica do inventário de cookies;

14.7.9.10. Permitir a geração de relatórios sobre uso e aceitação de cookies, segmentados por categoria, período e volume de usuários;

14.7.10. **Módulo 10 - Gestão de Aceites – este módulo deverá**:

14.7.10.1. Possibilitar a criação de formulários eletrônicos de consentimento, personalizáveis por finalidade de tratamento de dados;

14.7.10.2. Permitir incluir cláusulas específicas, campos obrigatórios e opcionais, bem como caixas de seleção (opt-in) para cada finalidade;

14.7.10.3. Possibilitar a inclusão de campos adicionais definidos pelo controlador;

14.7.10.4. Permitir a inserção de textos orientativos explicando a finalidade da coleta e as consequências da não concessão do consentimento;

14.7.10.5. Armazenar cada aceite em banco de dados, vinculando-o ao titular, com, no mínimo, registro de data, hora, IP/dispositivo, versão do termo e finalidade;

14.7.10.6. Permitir consulta individual ou em massa dos consentimentos concedidos;

14.7.10.7. Permitir exportar relatórios com todos os consentimentos para auditoria ou comprovação legal;

14.7.10.8. Possibilitar que o titular consulte e retire seu consentimento a qualquer momento, por meio de link ou portal disponibilizado;

14.7.10.9. Permitir o registro da revogação, com data e justificativa, preservando o histórico de aceites anteriores;

14.7.10.10. Permitir configurar prazos de retenção e alertar quando determinado consentimento estiver prestes a expirar;

14.7.10.11. Permitir a geração de relatórios sobre quantidade de consentimentos concedidos/revogados por finalidade;

14.7.10.12. Possibilitar exportação em formatos XLS e PDF.

14.7.11. **Módulo 11 - Gestão de Documentos – este módulo deve**:

14.7.11.1. Permitir o cadastro de novos documentos, com preenchimento de campos obrigatórios como: título, descrição, tipo de documento, área e responsável;

14.7.11.2. Possibilitar o upload de arquivos, armazenando-os em repositório centralizado, garantindo segurança e rastreabilidade;

14.7.11.3. Permitir que documentos sejam classificados como ativos ou obsoletos, mantendo sempre o histórico preservado;

14.7.11.4. Manter histórico completo das versões de cada documento, com registro de data, autor e justificativa da revisão;

14.7.11.5. Possibilitar a visualização, comparação e restauração de versões anteriores;

14.7.11.6. Permitir que documentos obsoletos fiquem inativos, mas preservando sua rastreabilidade para consulta futura;

14.7.11.7. Possibilitar a tramitação de documentos em fluxo de aprovação, definido previamente conforme perfis e hierarquia de aprovadores;

14.7.11.8. Notificar automaticamente os aprovadores sobre documentos pendentes de análise;

14.7.11.9. Permitir que aprovadores realizem as seguintes ações:

14.7.11.9.1. Aprovar o documento, com registro de assinatura digital;

14.7.11.9.2. Rejeitar o documento, retornando-o ao criador com justificativa obrigatória.

14.7.11.10. Garantir que, uma vez aprovado por todos os aprovadores, o documento seja automaticamente publicado como versão válida, acessível conforme permissões definidas;

14.7.11.11. Permitir que o controle de acesso seja configurado tanto em nível macro, por categoria ou tipo documental, quanto em nível micro, por documento individual, assegurando flexibilidade na gestão das permissões de visualização, edição, tramitação e aprovação;

14.7.11.12. Permitir que documentos aprovados sejam revisados a qualquer momento mediante justificativa;

14.7.11.13. Gerar nova versão do documento em revisão, que deverá tramitar novamente pelo fluxo de aprovação antes da publicação;

14.7.11.14. Manter histórico detalhado das revisões realizadas, com identificação do responsável e data;

14.7.11.15. Possibilitar a emissão de relatórios sobre tramitação, aprovações, rejeições e versões;

14.7.11.16. Garantir rastreabilidade completa desde a criação até a publicação ou obsolescência do documento;

14.7.11.17. Preservar integridade, transparência e segurança da informação durante todo o ciclo de vida documental.

Serviço de consultoria especializada

14.8. A consultoria especializada deverá apoiar a organização no preenchimento dos módulos, através de auxílio metodológico e de uso da ferramenta:

14.9. A consultoria deverá ser executada através de atividades a serem desenvolvidas em reuniões, presenciais e/ou virtuais, devendo-se focar no detalhamento do plano de execução dos serviços, contemplando a metodologia de gestão, macro programa, plano de comunicação, relatórios de status e interfaces;

14.10. Nas reuniões de início deverão obrigatoriamente ser tratados os temas:

14.10.1. A LGPD e seus aspectos direcionados à Administração Pública;

14.10.2. A importância da conformidade para a CONTRATANTE;

14.10.3. O projeto de adequação;

14.10.4. O processo de construção do programa de conformidade com a LGPD;

14.10.5. A definição dos agentes envolvidos e seus respectivos papéis de acordo com a Lei Geral de Proteção de Dados.

14.11. As reuniões de planejamento entre CONTRATANTE e a CONTRATADA seguirão um cronograma a ser firmado em até 2 (dois) dias úteis após o início da prestação do serviço, dado o prazo exíguo da execução da fase, e poderão ser realizadas de forma remota, desde que acordado entre as partes;

14.12. Deverá ser apresentada a comprovação de aptidão profissional para desempenho de atividades pertinentes e compatíveis com este item, por meio de profissional tecnicamente habilitado (capacidade técnico-profissional), conforme a relação de perfis a seguir que identifica aqueles com conhecimentos imprescindíveis, considerando as tecnologias, metodologias e conhecimentos existentes nos ambientes e sistemas da CONTRATANTE;

14.13. Para cada um destes perfis, a LICITANTE deverá apresentar as comprovações de que os profissionais pertencem aos seus quadros (através de CTPS ou Contrato de Trabalho), ou que possui compromisso para a contratação destes colaboradores quando do início dos serviços (através de declaração de intenção de contratação da LICITANTE assinada pelo futuro colaborador). Além dos currículos e os certificados exigidos para cada perfil:

14.13.1. **01** Analista de sistemas.

14.13.1.1. Nível superior completo em áreas da Tecnologia da Informação.

14.13.2. **01** Advogado.

14.13.2.1. Nível superior completo em direito com registro na OAB.

14.13.3. **01** Analista de requisitos.

14.13.3.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito.

14.13.3.2. Título de especialização em engenharia de sistemas para web, gestão empresarial ou áreas afins.

14.13.4. **01** Analista de Segurança da informação.

14.13.4.1. Nível superior completo na área de Segurança da Informação.

14.13.5. **01** Analista de Governança Corporativa.

14.13.5.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

14.13.5.2. Título de especialização em governança corporativa e risco, ou áreas afins;

14.13.5.3. Certificação Lead Assessor SIG ISO 37301:2021 – Gestão em Compliance – Requisitos com orientações para uso;

14.13.5.4. Certificação Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019 – Gestão de Riscos e Continuidade de Negócios.

14.13.6. **01** Encarregado de Dados (DPO).

14.13.6.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação ou direito;

14.13.6.2. Certificação como Lead Assessor ISO 27001:2022 e ISO 27701:2019 – Gestão da Segurança da Informação e Gestão de Privacidade da Informação;

14.13.6.3. Certificação Data Protection Officer – DPO.

14.14. A qualificação mínima apresentada não é relacionada com o número de profissionais que compõem o projeto, podendo um mesmo profissional apresentar mais de uma qualificação que atenda ao exigido;

Terceirização do Encarregado de Dados (DPO)

14.15. A CONTRATADA deverá assumir as responsabilidades do Encarregado de Dados, prestando os serviços de acordo com o disposto na Lei nº 13.709/2018 – LEI GERAL DE PROTEÇÃO DE DADOS (LGPD), considerando as atividades e responsabilidades prestadas por esta, com base no artigo 41, parágrafo 2º, conforme o escopo de trabalho:

14.15.1. IMPLANTAÇÃO DAS NOVAS DIRETRIZES QUE SERÃO CRIADAS PELA AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS (ANPD): A empresa CONTRATADA ficará responsável por: 1) manter-se constantemente atualizada, em relação aos novos regulamentos e instruções normativas editados pela ANPD; 2) analisar com sua equipe de profissionais a legalidade ou não desses regulamentos; 3) apresentar orientações técnicas para CONTRATANTE sobre as formas de implementar as novas exigências que estejam de acordo com a LGPD e com a Constituição Federal;

14.15.2. ATENDIMENTO DE DEMANDAS DOS ÓRGÃOS DE FISCALIZAÇÃO DE ACORDO COM A LGPD: A CONTRATADA fica responsável por: 1) receber e responder, nos prazos legais, as demandas veiculadas por órgãos de fiscalização municipal, estadual e federal; 2) analisar a legalidade de eventuais exigências impostas; 3) apresentar orientações

técnicas para CONTRATANTE sobre as formas de implementar as novas exigências que estejam de acordo com a LGPD e com a Constituição Federal;

14.15.3. ATENDIMENTO DE DEMANDAS DO MINISTÉRIO PÚBLICO SOBRE A LGPD: A CONTRATADA fica responsável por: 1) receber e responder, nos prazos legais, todos os pedidos de informações dos Ministérios Públicos Federal, Estadual e do Trabalho; 2) analisar a legalidade de eventuais exigências feitas por esses órgãos; 3) apresentar orientações técnicas para CONTRATANTE sobre as formas de implementar as exigências legais feitas pelo ministério público;

14.15.4. ATENDIMENTO DAS DEMANDAS DOS TITULARES DOS DADOS: A CONTRATADA será responsável por: 1) Receber e responder, nos prazos legais, pedidos encaminhados pelos titulares dos dados; 2) analisar a legalidade e os riscos desses pedidos; 3) Auxiliar a CONTRATANTE na defesa contra pedidos abusivos;

14.15.5. ANÁLISE DE CONFORMIDADE DE PARCEIROS: A CONTRATADA será responsável por: 1) Avaliar a conformidade de parceiros da CONTRATANTE em relação à LGPD e à segurança de dados, através de auditorias e due diligence; 2) Orientar a CONTRATANTE quanto aos riscos envolvidos no contrato; 3) Disseminar os procedimentos de privacidade e proteção de dados a todas as partes interessadas.

14.16. Plataforma unificada de SERVIÇOS GERENCIADOS DE SEGURANÇA (MSS) com setup/implantação e suporte de 12 meses;

14.16.1. A proponente deverá obrigatoriamente atender integralmente e obrigatoriamente a todos os requisitos detalhados em cada um dos itens da plataforma, garantindo uma postura de segurança robusta e abrangente em todo o ambiente da CONTRATANTE;

14.16.2. A solução deverá ser ofertada na modalidade Software como Serviço (SaaS), centralizada em nuvem própria da contratada, no modelo SaaS, hospedada em infraestrutura própria ou On Premise ficando a criterio da Contratante optar por qual modalidade ira implantar;

14.16.3. Compõem os serviços gerenciados de segurança da informação (MSS):

14.16.3.1. A solução proposta no item 10 deverá consolidar todas as funcionalidades em uma plataforma automatizada, unificada e integrada, acessível através de um único painel de gestão centralizado. Esta abordagem elimina a complexidade de gerenciar ferramentas de segurança díspares, permitindo que a equipe de segurança monitore, configure e responda a incidentes de forma coesa e eficiente.

14.16.3.2. A solução proposta no item 10 deverá ter um único painel de controle ou “dashboard”, um único agente, um único mecanismo ou “motor” para proteger, detectar e responder automaticamente a mais de 92% dos “tickets”/chamados criados nos 14 módulos de cibersegurança e governança de dados. Graças a esse mecanismo único, é possível correlacionar as ações realizadas em todos os módulos e consolidá-las em um único chamado e painel de controle e devera conter obrigatoriamente os seguintes módulos:

14.16.3.2.1. **Módulo de Segurança de Nuvem**:

14.16.3.2.1.1. Deverá permitir integração com provedores SaaS como Microsoft 365, Google Workspace, Salesforce, Box, Dropbox e Slack por meio de APIs nativas com autenticação OAuth2.0 e suporte a SCIM;

14.16.3.2.1.2. Deverá oferecer varredura automatizada de arquivos em repouso, trânsito e compartilhados, com detecção de malware, ransomware e exploits baseados em análise comportamental e assinatura;

14.16.3.2.1.3. Deve ter capacidade de identificar atividades anômalas com base em aprendizado de máquina e gerar automaticamente tickets para aplicações em nuvem ao detectar atividade administrativa fora do padrão, violação nas permissões de acesso, detecção de malware em armazenamento na nuvem, exclusão massiva de dados, download massivo de dados, indícios de ataques automatizados (bots) e potencial comprometimento de identidade;

14.16.3.2.1.4. Deverá implementar políticas de acesso condicional baseadas em identidade, localização geográfica e IP com bloqueio automático;

14.16.3.2.1.5. Deverá permitir criação de workflows automatizados de resposta a incidentes, com ações como isolamento de arquivos, revogação de permissões e notificação a administradores;

14.16.3.2.1.6. Deverá registrar logs de auditoria completos para todas as ações realizadas via integração em nuvem, com retenção mínima de 365 dias;

14.16.3.2.1.7. Deverá ser compatível com normativas como GDPR, HIPAA e SOC 2, com geração de relatórios de conformidade;

14.16.3.2.1.8. Deverá permitir integração com sistemas de SIEM (como Splunk e QRadar) via API RESTful e/ou exportação de logs em formato JSON e syslog;

14.16.3.2.1.9. Deverá oferecer visualização de postura de segurança dos usuários e aplicações conectadas, com classificação de risco;

14.16.3.2.1.10. Deverá permitir configuração de regras de DLP (Data Loss Prevention) com detecção de dados sensíveis como PII, PHI, PCI e dados regulatórios customizados por regex, com notificações em tempo real por e-mail e webhook;

14.16.3.2.1.11. Deverá suportar autenticação multifator (MFA) para administradores e usuários com privilégios elevados;

14.16.3.2.1.12. Deverá ser capaz de bloquear sessões ativas e revogar tokens de acesso automaticamente em caso de detecção de violação;

14.16.3.2.1.13. Deverá prover um painel unificado (dashboard) com visualização por tenant, aplicativo, tipo de incidente e usuário afetado;

14.16.3.2.1.14. Deverá permitir granularidade de permissões administrativas (RBAC), com auditoria das ações realizadas por cada perfil;

14.16.3.2.1.15. Deverá oferecer compatibilidade com SAML 2.0 e OpenID Connect para autenticação federada;

14.16.3.2.1.16. Deverá manter status de integridade das conexões com aplicativos em nuvem, alertando em caso de perda de sincronização ou erro de API.

14.16.3.3. **Módulo de Segurança de E-mail**

14.16.3.3.1. Deverá ter integração nativa com Gmail e Microsoft 365 por meio de APIs seguras com autenticação baseada em OAuth 2.0, permitindo varredura de e-mails em tempo real;

14.16.3.3.2. Deverá ser capaz de detectar e bloquear ameaças como malware, ransomware, spear-phishing, spoofing e business email compromise (BEC), utilizando análise comportamental e assinaturas dinâmicas;

14.16.3.3.3. A plataforma deve ter um sistema de quarentena automática e manual com ações configuráveis por nível de risco e tipo de ameaça;

14.16.3.3.4. Deverá permitir a visualização de todos os e-mails inspecionados, indicando ações tomadas (permitido, bloqueado, sinalizado) e risco classificado por cor;

14.16.3.3.5. Deverá ter recursos de marcação de e-mails suspeitos (“warn recipients”) em vez de bloqueio direto, com destaque visual embutido no conteúdo;

14.16.3.3.6. Deverá permitir que administradores configurem políticas de escaneamento com granularidade por domínio, grupo e usuário;

14.16.3.3.7. Deverá permitir a criação de listas de bloqueio (denylist) e de permissões (allowlist) com base em IP, domínio, endereço de e-mail e remetente autenticado (SPF/DKIM/DMARC);

14.16.3.3.8. Deverá permitir a visualização e o gerenciamento de todos os tickets de e-mail gerados, com possibilidade de reabertura, exclusão, download do arquivo de e-mail e comentários administrativos;

14.16.3.3.9. Deverá registrar logs detalhados de cada mensagem processada, incluindo cabeçalhos, anexos, remetente e destinatário;

14.16.3.3.10. Deverá permitir integração com ferramentas de auditoria, SIEM e MDR via exportação de logs (JSON/syslog) e APIs RESTful;

14.16.3.3.11. Deverá oferecer simulações de campanhas de phishing realistas e relatórios de engajamento para reforço da conscientização dos usuários, em conjunto com o módulo de conscientização;

14.16.3.3.12. Deverá permitir exportação de relatórios de incidentes por tipo de ameaça, remetente, usuário afetado e ação tomada, com filtros por período;

14.16.3.3.13. Deverá integrar-se ao módulo de mensagens seguras para envio criptografado de mensagens de saída, com logs de leitura e controle de expiração;

14.16.3.3.14. Deverá suportar mensagens assinadas digitalmente (S/MIME) e garantir a integridade de e-mails internos por verificação de identidade;

14.16.3.3.15. Deverá ter complementos opcionais para Outlook e Gmail que permitam o reporte direto de e-mails suspeitos pelos usuários, com criação automática de tickets;

14.16.3.3.16. Deverá atualizar suas definições de ameaças em tempo real, com base em feed de inteligência global, análises heurísticas e engine LLM de classificação.

14.16.3.4. **Módulo de Segurança de Endpoint**

14.16.3.4.1. Deverá ter um agente leve compatível com Windows, macOS e Linux, com capacidade de operação mesmo offline, realizando coleta e resposta local;

14.16.3.4.2. Deverá realizar varredura contínua em tempo real no sistema de arquivos, memória e rede local em busca de comportamentos maliciosos ou arquivos suspeitos;

14.16.3.4.3. Deverá incluir controle de execução de aplicações, permitindo bloqueio por hash, nome, assinatura digital e tipo de arquivo;

14.16.3.4.4. Deverá oferecer detecção baseada em inteligência artificial e aprendizado de máquina com análise comportamental para arquivos desconhecidos e execução anômala de processos;

14.16.3.4.5. Deverá registrar atividades de sistema como criação de processos, conexões de rede, alterações em arquivos críticos e instalação de drivers;

14.16.3.4.6. Deverá permitir a aplicação de políticas por grupo, perfil de risco e tipo de dispositivo, com herança e exceções configuráveis;

14.16.3.4.7. Deverá suportar gestão remota de endpoints, incluindo execução de comandos, scripts e atualizações, mesmo fora da rede corporativa;

14.16.3.4.8. Deverá manter inventário completo de hardware, sistema operacional e software em cada endpoint;

14.16.3.4.9. Deverá gerar alertas em tempo real, via painel, e-mail e API, com criticidade definida por tipo de ameaça e impacto no endpoint;

14.16.3.4.10. Deverá permitir quarentena automática ou manual de arquivos suspeitos, com opção de recuperação segura ou exclusão permanente;

14.16.3.4.11. Deverá suportar logs exportáveis em formatos compatíveis com SIEM (JSON, syslog, CEF) e integração direta via API.

14.16.3.5. **Módulo de Governança de Dados em Endpoints**

14.16.3.5.1. Deverá monitorar continuamente arquivos armazenados nos dispositivos, identificando dados sensíveis como PII, PHI, informações financeiras e dados regulatórios (como LGPD, HIPAA, PCI), com uso de padrões pré-definidos e expressões regulares personalizadas;

14.16.3.5.2. Deverá classificar automaticamente os dados em categorias de sensibilidade, origem e risco, com base em conteúdo e contexto de uso;

14.16.3.5.3. Deverá permitir definir políticas de controle de acesso e movimentação de dados sensíveis, incluindo bloqueio de cópia para mídias removíveis e upload não autorizado;

14.16.3.5.4. Deverá identificar tentativas de exfiltração de dados via USB, e-mail, ferramentas de sincronização em nuvem (como Dropbox, OneDrive e Google Drive) e redes ponto a ponto;

14.16.3.5.5. A plataforma deve oferecer recurso de detecção de uso não autorizado de aplicações (shadow IT) e bloqueio de aplicações não autorizadas que manipulam dados locais;

14.16.3.5.6. Deverá suportar criptografia de arquivos confidenciais em endpoints, com controle central de chaves e rastreamento de acessos;

14.16.3.5.7. A solução deverá alertar administradores em tempo real sobre movimentações não autorizadas de dados, incluindo upload para domínios não confiáveis ou cópia para dispositivos externos;

14.16.3.5.8. Deverá integrar-se com DLP de e-mail e nuvem para políticas unificadas de governança de dados em múltiplos vetores, permitindo geolocalização de dispositivos e rastreamento da origem de movimentações de dados sensíveis;

14.16.3.5.9. Deverá ter painéis de risco por endpoint, usuário e tipo de dado sensível encontrado, com filtros por período, severidade e conformidade;

14.16.3.5.10. Deverá permitir aplicar políticas diferenciadas por perfil de usuário, grupo de diretório, departamento ou classificação de risco;

14.16.3.5.11. Deverá registrar todos os eventos de governança de dados em formato exportável para SIEM (JSON, syslog), com registro de data, hora e identificadores únicos;

14.16.3.5.12. Deverá suportar alertas e relatórios automatizados via e-mail e APIs externas (como Slack, Teams e ServiceNow);

14.16.3.5.13. Deverá ser compatível com criptografia nativa de sistema operacional (BitLocker, FileVault) para orquestração de segurança de dados.

14.16.3.6. **Módulo de Governança de Dados**

14.16.3.6.1. Deverá permitir a análise contínua de dados associados a contas de usuário, identificando conteúdos sensíveis acessados, compartilhados ou modificados, tanto em dispositivos quanto em nuvem;

14.16.3.6.2. Deverá aplicar políticas de DLP (Data Loss Prevention) com base em identidade, considerando o comportamento histórico do usuário e o contexto da ação;

14.16.3.6.3. Deverá detectar e alertar sobre movimentações anômalas de dados feitas por contas com privilégios elevados, inclusive administradores de sistema e usuários com acesso a dados regulados;

14.16.3.6.4. Deverá integrar-se com Active Directory, Azure AD e Google Workspace, permitindo a sincronização automática de perfis, grupos e permissões;

14.16.3.6.5. Deverá identificar compartilhamento de arquivos sensíveis por usuários com terceiros, seja por e-mail, links públicos ou uploads não autorizados;

14.16.3.6.6. Deverá permitir respostas como revogação de permissões, bloqueio de conta, encerramento de sessão ou quarentena de dados manipulados;

14.16.3.6.7. Deverá possuir um dashboard com visão consolidada por usuário, destacando interações com dados sensíveis, dispositivos, apps conectados e volume de tráfego;

14.16.3.6.8. Deverá bloquear ou alertar sobre tentativas de upload de documentos confidenciais para domínios externos ou serviços não autorizados;

14.16.3.6.9. Deverá alertar sobre padrões suspeitos de login e movimentação de arquivos, incluindo logins simultâneos de locais distintos;

14.16.3.6.10. Deverá disponibilizar notificações via e-mail, webhook;

14.16.3.6.11. Deverá suportar integração com SIEMs para envio de incidentes correlacionados a identidade e exportação de score de risco por usuário.

14.16.3.7. **Módulo de Segurança de Rede**

14.16.3.7.1. Deverá permitir monitoramento contínuo do tráfego de rede em endpoints protegidos, identificando comunicações com domínios maliciosos, botnets, infraestrutura de comando e controle e endereços de IP de reputação negativa;

14.16.3.7.2. Deverá aplicar inspeção de pacotes em tempo real para identificar tentativas de exfiltração, túneis encobertos, varredura de portas e movimentação lateral;

14.16.3.7.3. Deverá ter proteção contra sequestro de consultas DNS e permitir o redirecionamento seguro de consultas para servidores confiáveis;

14.16.3.7.4. Deverá integrar-se com SIEMs e firewalls para envio e recepção de alertas de rede, bloqueios automáticos e auditoria de tráfego;

14.16.3.7.5. Deverá inspecionar conexões seguras (TLS/SSL) utilizando informações de nome de servidor e certificado digital para detectar comunicação com destinos maliciosos;

14.16.3.7.6. Deverá registrar logs completos de sessões de rede com endereço de origem e destino, portas, protocolos, data, hora e nome da aplicação;

14.16.3.7.7. Deverá suportar resposta automatizada a incidentes de rede, como encerramento de processos, descarte de pacotes, bloqueio de endereços IP ou geração de alerta;

14.16.3.7.8. Deverá manter inventário de endereços IP utilizados por dispositivos protegidos, com histórico de alterações e localização;

14.16.3.7.9. Deverá permitir configuração de perfis de rede confiáveis e não confiáveis para controle de políticas adaptativas;

14.16.3.7.10. Deverá permitir rastreabilidade de incidentes de rede com linha do tempo, gráficos e correlação com outras camadas de segurança.

14.16.3.8. **Módulo de Gestão de Equipamentos Móveis (MDM)**

14.16.3.8.1. Deverá possibilitar cadastro e gerenciamento centralizado de dispositivos móveis (iOS e Android), incluindo perfis, configurações e status de conformidade;

14.16.3.8.2. Deverá aplicar políticas de segurança móveis, como bloqueio remoto, limpeza seletiva de dados e criptografia de dados em repouso;

14.16.3.8.3. Deverá permitir inventário detalhado dos dispositivos, incluindo versões de sistema, aplicativos instalados, correções e configurações de segurança;

14.16.3.8.4. Deverá monitorar continuamente o status de conformidade dos dispositivos, alertando administradores sobre desvios de política;

14.16.3.8.5. Deverá suportar controle de aplicativos permitidos e bloqueados, incluindo listas de permissão e de bloqueio para aplicativos móveis;

14.16.3.8.6. Deverá permitir geolocalização e rastreamento em tempo real dos dispositivos móveis cadastrados;

14.16.3.8.7. A solução deverá permitir o envio remoto de comandos para bloqueio, desbloqueio e redefinição dos dispositivos;

14.16.3.8.8. Deverá oferecer painéis com métricas sobre segurança, conformidade e uso dos dispositivos móveis;

14.16.3.8.9. Deverá suportar políticas de atualização automática de sistema operacional e aplicativos autorizados;

14.16.3.8.10. Deverá permitir gerenciamento de perfis de rede privada virtual e redes sem fio para dispositivos móveis, garantindo conexões seguras;

14.16.3.8.11. Deverá suportar a segregação de dados corporativos e pessoais (containerização) em dispositivos de uso misto;

14.16.3.8.12. Deverá enviar alertas em tempo real para administradores sobre incidentes de segurança nos dispositivos móveis;

14.16.3.8.13. Deverá permitir integração com sistemas SIEM para envio e análise de eventos de dispositivos móveis;

14.16.3.8.14. Deverá oferecer suporte a múltiplos administradores com controle granular de permissões para gerenciamento móvel;

14.16.3.8.15. Deverá suportar integração com sistemas de controle de chamados para gerenciamento eficiente de incidentes móveis.

14.16.3.9. **Módulo de Endpoint Detection and Response (EDR)**

14.16.3.9.1. Deverá realizar monitoramento contínuo de endpoints para detecção de comportamentos suspeitos e indicadores de ataque em tempo real;

14.16.3.9.2. Deverá aplicar técnicas avançadas de análise comportamental para identificar ameaças zero-day e ataques sofisticados;

14.16.3.9.3. A plataforma deve integrar-se com fontes de inteligência de ameaças para atualização automática de assinaturas e indicadores de comprometimento (IOCs);

14.16.3.9.4. Possibilitar investigação forense remota, incluindo coleta de evidências e análise detalhada de eventos;

14.16.3.9.5. Suportar resposta automatizada a incidentes, como isolamento de dispositivo, bloqueio de processo e quarentena de arquivos;

14.16.3.9.6. Manter histórico completo dos eventos e respostas para auditoria e conformidade regulatória;

14.16.3.9.7. Permitir criação e customização de regras de detecção para adequação a diferentes ambientes;

14.16.3.9.8. Disponibilizar dashboards e relatórios detalhados sobre o status de segurança dos endpoints;

14.16.3.9.9. Integrar-se com sistemas SIEM e SOAR para automação e correlação de incidentes;

14.16.3.9.10. Oferecer suporte multiplataforma, incluindo Windows, macOS e Linux;

14.16.3.9.11. Identificar e bloquear comportamentos de ransomware em tempo real;

14.16.3.9.12. Alertar sobre acesso não autorizado a dados sensíveis ou sistemas críticos;

14.16.3.9.13. Possibilitar quarentena automático e manual de arquivos suspeitos;

14.16.3.9.14. Suportar integração com ferramentas de ticketing para gerenciamento eficiente de incidentes;

14.16.3.9.15. Deverá oferecer visibilidade completa dos processos ativos e conexões de rede nos endpoints.

14.16.3.10. **Módulo de Inbound Gateway**

14.16.3.10.1. Deverá atuar como gateway de e-mail, interceptando todas as mensagens recebidas antes da entrega ao servidor interno;

14.16.3.10.2. Deverá aplicar análise de conteúdo e reputação para cada e-mail, verificando anexos, links e remetentes;

14.16.3.10.3. Deverá suportar autenticações SPF, DKIM e DMARC, rejeitando e-mails que não passam nas verificações;

14.16.3.10.4. Deverá bloquear mensagens com arquivos executáveis, scripts ou formatos potencialmente perigosos;

14.16.3.10.5. Deverá identificar e mitigar ataques de spoofing, comprometimento de e-mail corporativo e phishing;

14.16.3.10.6. Deverá suportar detecção e neutralização de e-mails com links maliciosos, encurtadores e redirecionamentos;

14.16.3.10.7. Deverá manter quarentena gerenciável pelo usuário com opção de liberar, excluir ou reportar falso positivo;

14.16.3.10.8. A plataforma deve oferecer console de administração com logs completos e rastreabilidade de e-mails por usuário;

14.16.3.10.9. Deverá integrar-se com diretórios como Active Directory, Azure AD e Google Workspace para aplicação de políticas por grupo;

14.16.3.10.10. Deverá oferecer filtros de linguagem ofensiva, informações sensíveis e termos configuráveis;

14.16.3.10.11. Deverá permitir integração com SIEMs para envio de alertas e eventos de segurança relacionados a e-mail.

14.16.3.11. **Módulo de Secure Web Gateway**

14.16.3.11.1. A plataforma deve atuar como proxy seguro para o tráfego web dos usuários, monitorando, filtrando e registrando o acesso a sites e serviços online;

14.16.3.11.2. A solução deverá aplicar políticas de bloqueio de categorias de sites, como pornografia, jogos e redes sociais, com base em perfis de usuário;

14.16.3.11.3. Deverá suportar filtragem de URLs com base em reputação, listas de bloqueio e palavras-chave;

14.16.3.11.4. Deverá gerar logs detalhados de navegação por usuário, dispositivo, domínio acessado e horário;

14.16.3.11.5. Deverá permitir aplicação de políticas diferenciadas por grupo de diretório, departamento ou perfil de risco;

14.16.3.11.6. Deverá oferecer alertas em tempo real sobre tentativas de acesso a sites suspeitos ou bloqueados;

14.16.3.11.7. Deverá suportar integração com ferramentas SIEM para envio de eventos e geração de alertas correlacionados;

14.16.3.11.8. Deverá permitir exceção de inspeção de tráfego seguro para domínios confiáveis e serviços essenciais;

14.16.3.11.9. Deverá identificar tentativas de evasão por meio de proxies, redes privadas virtuais e serviços de anonimato;

14.16.3.11.10. Deverá bloquear conexões para domínios recém-criados ou com baixa reputação;

14.16.3.11.11. Deverá suportar acesso remoto seguro à web via proxy em nuvem ou cliente de rede privada virtual leve;

14.16.3.11.12. Deverá manter política de retenção de logs por período configurável para auditoria;

14.16.3.11.13. Deverá permitir geração de relatórios periódicos sobre uso da web, sites acessados e riscos detectados;

14.16.3.11.14. Deverá fornecer painel centralizado para gerenciamento e ajuste dinâmico das políticas de navegação;

14.16.3.12. **Módulo de Wi-Fi Phishing**

14.16.3.12.1. A plataforma deve detectar tentativas de criação de redes Wi-Fi falsas (evil twin) que simulam SSIDs corporativos;

14.16.3.12.2. A solução deverá alertar automaticamente quando dispositivos corporativos se conectarem a redes sem fio não autorizadas;

14.16.3.12.3. A plataforma deve permitir criação de políticas para impedir conexões a redes abertas ou inseguras;

14.16.3.12.4. A solução deverá realizar varreduras passivas e ativas para identificar pontos de acesso maliciosos próximos aos usuários;

14.16.3.12.5. A plataforma deve registrar identificadores de rede, endereços de hardware, localizações e horários de tentativas de phishing via redes sem fio;

14.16.3.12.6. A solução deverá aplicar heurísticas de detecção com base em nome de rede, força de sinal e comportamento de conexão;

14.16.3.12.7. A plataforma deve gerar alertas em tempo real para a equipe de segurança sobre conexões potencialmente perigosas;

14.16.3.12.8. A plataforma deve manter histórico de redes conectadas por cada dispositivo, com dados sobre risco associado;

14.16.3.12.9. A solução deverá identificar pontos de acesso com nomes semelhantes aos da empresa, mas operando em canais ou locais diferentes;

14.16.3.12.10. A plataforma deve permitir integração com SIEM para envio de alertas de Wi-Fi phishing e rastreamento de incidentes;

14.16.3.12.11. A plataforma deve suportar listas de redes sem fio confiáveis para aplicar políticas de permissão automáticas;

14.16.3.12.12. A solução deverá bloquear automaticamente comunicações de rede via interfaces sem fio em ambientes de alto risco;

14.16.3.12.13. A plataforma deve permitir configuração de notificações para o usuário final ao detectar tentativa de conexão insegura;

14.16.3.12.14. A plataforma deve identificar mudanças repentinas de identificador de hardware em redes conhecidas como potencial sinal de ataque;

14.16.3.12.15. A solução deverá ser compatível com diferentes fabricantes de hardware e conjuntos de chips de rede sem fio usados nos dispositivos da organização.

14.16.3.13. **Módulo de Segurança de Mensagens**

14.16.3.13.1. Deverá permitir o envio de mensagens criptografadas ponto a ponto entre usuários corporativos e externos;

14.16.3.13.2. Deverá garantir que apenas o destinatário pretendido consiga acessar o conteúdo da mensagem;

14.16.3.13.3. Deverá oferecer autenticação de destinatário via senha, código temporário ou autenticação federada;

14.16.3.13.4. Deverá permitir controle de expiração automática da mensagem após tempo configurável;

14.16.3.13.5. Deverá suportar a revogação de acesso a mensagens já enviadas, com bloqueio retroativo;

14.16.3.13.6. Deverá registrar auditoria completa das ações na mensagem, incluindo leitura, encaminhamento e tempo de visualização;

14.16.3.13.7. Deverá impedir cópia, encaminhamento ou download não autorizado do conteúdo enviado;

14.16.3.13.8. Deverá integrar-se com plataformas de e-mail corporativo como Outlook, Gmail e interfaces web;

14.16.3.13.9. Deverá suportar envio seguro de anexos com criptografia granular e registros de acesso;

14.16.3.13.10. Deverá permitir personalização de marca na interface de mensagens seguras, incluindo logotipo, cores e remetente;

14.16.3.13.11. Deverá manter conformidade com requisitos regulatórios como GDPR, HIPAA e LGPD;

14.16.3.13.12. Deverá permitir envio em massa de mensagens criptografadas com gerenciamento por lote;

14.16.3.13.13. Deverá emitir alertas ao remetente sobre tentativas de acesso não autorizado ao conteúdo;

14.16.3.13.14. Deverá permitir anexar políticas de confidencialidade e termos de uso personalizados na mensagem;

14.16.3.13.15. Deverá permitir integração via API para envio programático de mensagens seguras por sistemas internos;

14.16.3.13.16. Deverá disponibilizar relatórios periódicos sobre mensagens seguras enviadas, lidas, expiradas e acessadas;

14.16.3.13.17. Deverá impedir que mensagens seguras sejam indexadas por motores de busca ou armazenadas em cache local.

14.16.3.14. **Módulo de Conscientização de Segurança**

14.16.3.14.1. O módulo de Treinamento de Conscientização de Segurança devera aprimorar a compreensão dos usuários sobre ameaças comuns à segurança, inscrevendo-os em planos de treinamento;

14.16.3.14.2. Deverá testar as simulações de phishing por e-mail para testar o nível de conscientização;

14.16.3.14.3. Deverá ter cursos de treinamento específicos para educar os usuários sobre as melhores práticas de cibersegurança;

14.16.3.14.4. A solução deverá ser ofertada na modalidade Software como Serviço (SaaS), centralizada em nuvem própria da contratada, no modelo SaaS, hospedada em infraestrutura própria;

14.16.3.14.5. Deverá contar com ambiente operacional em português do Brasil (pt-br);

14.16.3.14.6. Acesso total à plataforma de conscientização;

14.16.3.14.7. Disponibilizar APIs para exportação contínua de dados (maturidade, cursos, certificados, resultados de phishing, etc);

14.16.3.14.8. Atualizações, novos conteúdos e correções deverão ser disponibilizados sem custo adicional;

14.16.3.14.9. Permitir acessos simultâneos conforme o número de licenças adquiridas;

14.16.3.14.10. Arquitetura multi-tenant, permitindo administração simultânea de múltiplos administradores sob a mesma instância, com gestão segmentada e segura;

14.16.3.14.11. Gestão de campanhas de conscientização e simulações de phishing, com segmentação por grupos, perfis de risco e comportamento dos usuários;

14.16.3.14.12. Permitir a criação de conteúdo customizado em formato "newsletters";

14.16.3.14.13. Geração de Campanhas ilimitadas de phishing e conscientização realizadas pela equipe da CONTRATANTE;

14.16.3.14.14. Integração com SIEM;

14.16.3.14.15. Disponibilização contínua de atualizações de conteúdo, funcionalidades e melhorias da plataforma, sem custo adicional para o Contratante;

14.16.3.14.16. **CONTEÚDO.**

14.16.3.14.17. A biblioteca deverá contemplar conteúdos específicos voltados, no mínimo, para os seguintes tópicos:

14.16.3.14.17.1. dispositivos móveis;

14.16.3.14.17.2. inteligência artificial;

14.16.3.14.17.3. privacidade e proteção de dados;

14.16.3.14.17.4. redes sociais;

14.16.3.14.17.5. segurança de e-mail;

14.16.3.14.17.6. senhas e autenticação, trabalho remoto e redes Wi-Fi.

14.16.3.14.18. Deverá haver conteúdo específico voltado à Lei Geral de Proteção de Dados Pessoais (LGPD) brasileira e demais legislações correlatas;

14.16.3.14.19. Os conteúdos deverão ser entregues em formatos diversos, incluindo:

14.16.3.14.19.1. Vídeos;

14.16.3.14.19.2. Quizzes;

14.16.3.14.19.3. Infográficos;

14.16.3.14.19.4. trilhas de aprendizagem;

14.16.3.14.19.5. vídeos em formato novela;

14.16.3.14.19.6. pôsteres e assessments (avaliações).

14.16.3.14.20. A plataforma deverá possibilitar a carga e aceite de políticas e normas de segurança da informação definidas pelo Contratante;

14.16.3.14.21. A plataforma deverá oferecer caminhos de aprendizado personalizados, com base no perfil de risco e comportamento de cada usuário;

14.16.3.14.22. O conteúdo deverá estar em conformidade com metodologias de psicosegurança cibernética, utilizando inteligência artificial para adaptar os treinamentos ao contexto regulatório, cultural e operacional do CONTRATANTE;

14.16.3.14.23. A plataforma deverá disponibilizar módulos de gamificação, com uso de trilhas de aprendizado, perguntas interativas e personagens, visando aumentar o engajamento dos usuários;

14.16.3.14.24. Manter histórico por usuário e por campanha;

14.16.3.14.25. Permitir que os usuários sejam testados e instruídos instantaneamente sobre os indicativos fraudulentos da simulação;

14.16.3.14.26. Possibilitar a criação automatizada de um programa personalizado em segurança da informação, ou recomendação automática de treinamentos, considerando o nível de risco de cada usuário.

14.16.3.14.27. **USUÁRIO**

14.16.3.14.28. Permitir carga de usuários via arquivo .CSV;

14.16.3.14.29. Integrar-se com Active Directory (AD), Azure AD, Google Workspace ou Okta;

14.16.3.14.30. Prover gerenciamento de usuários e cursos, com possibilidade de seleção de módulos por grupo;

14.16.3.14.31. Atribuir treinamentos automaticamente para novos usuários;

14.16.3.14.32. Criar grupos de usuários com base no comportamento frente às simulações e treinamentos, com atribuição automática conforme este comportamento;

14.16.3.14.33. Inativar usuários sem perda do histórico de dados;

14.16.3.14.34. Caso não seja possível manter o histórico, a plataforma deverá prover meios de exportação em formato .CSV;

14.16.3.14.35. Permitir a transferência de licenças de usuários desligados para novos usuários;

14.16.3.14.36. Disponibilizar ambiente de gestão para acompanhamento online da progressão e desempenho dos usuários;

14.16.3.14.37. Disponibilizar perfis de acesso diferenciados para campanhas e treinamentos;

14.16.3.14.38. Possibilitar autenticação em dois fatores para usuários e administradores;

14.16.3.14.39. Disponibilizar portal individual para cada funcionário, com atividades pendentes, histórico de treinamentos, troféus conquistados, ranking com demais colaboradores e conteúdos adicionais autorizados;

14.16.3.14.40. Permitir recuperação de senha segura pelo próprio usuário;

14.16.3.14.41. Possibilitar a segmentação automática de usuários que interagirem com campanhas de phishing, direcionando-os a treinamentos específicos;

14.16.3.14.42. **ALERTAS E NOTIFICAÇÕES**

14.16.3.14.43. Disparo automático de e-mails para usuários incluídos em novas campanhas;

14.16.3.14.44. Disparo automático de lembretes para usuários com treinamentos pendentes;

14.16.3.14.45. Disparo automático de notificações para gestores sobre funcionários com treinamentos pendentes;

14.16.3.14.46. Disparo automático de alertas para administradores da solução, com listagem de pendências;

14.16.3.14.47. **GESTÃO**

14.16.3.14.48. Disponibilizar painel gerencial com porcentagem de inscrições, cursos iniciados, concluídos e pendentes;

14.16.3.14.49. Disponibilizar relatórios executivos e de gestão sobre campanhas e treinamentos;

14.16.3.14.50. Permitir a emissão de certificados personalizados com a identidade visual do Contratante;

14.16.3.14.51. Apresentar painel de grau de maturidade em segurança da informação, por usuário e por área, considerando treinamentos concluídos e testes de phishing;

14.16.3.14.52. **DISPONIBILIDADE**

14.16.3.14.53. Garantir disponibilidade mínima de 99% mensal;

14.16.3.14.54. Indisponibilidades deverão ser informadas com 24h de antecedência e ocorrer fora do horário comercial, exceto em urgências;

14.16.3.14.55. Acesso à plataforma deve ser possível via navegador (compatível com Google Chrome, no mínimo);

14.16.3.14.56. **RELATÓRIOS**

14.16.3.14.57. Disponibilizar relatórios que demonstrem: usuários que receberam campanhas, concluíram treinamentos, possuem atividades pendentes, com filtros por campanha, período e grupos;

14.16.3.14.58. Relatórios personalizados e dinâmicos das campanhas, com filtros por campanha, período, grupo de usuários, nível de risco e status de conclusão de treinamentos;

14.16.3.14.59. Relatórios incluindo, no mínimo: maturidade em segurança da informação por usuário e por organização, perfis de risco individuais, indicadores de engajamento, métricas de simulação de phishing (incluindo taxa de abertura, cliques e reportes), evolução de conformidade (LGPD, ISO 27001, etc.) e grau de efetividade das campanhas de treinamento;

14.16.3.14.60. Relatórios exportáveis em múltiplos formatos (CSV, PDF, API) para integração com sistemas internos do Contratante;

14.16.3.14.61. Emissão de um (01) relatório executivo e operacional para gestores administradores, além de emissão de certificados digitais vinculados à conclusão de treinamentos com a identidade visual do Contratante;

14.16.3.14.62. **CONFORMIDADE REGULATÓRIA AUTOMATIZADA**

14.16.3.14.63. A plataforma deverá automatizar treinamentos e relatórios de conformidade em segurança da informação, atendendo requisitos da LGPD, PDPA e ISO 27001, facilitando auditorias internas e externas e garantindo compliance contínuo;

Módulo de Endpoint Detection and Response (EDR)

14.17. Deverá realizar monitoramento contínuo de endpoints para detecção de comportamentos suspeitos e indicadores de ataque em tempo real;

14.18. Deverá aplicar técnicas avançadas de análise comportamental para identificar ameaças zero-day e ataques sofisticados;

14.19. A plataforma deve integrar-se com fontes de inteligência de ameaças para atualização automática de assinaturas e indicadores de comprometimento (IOCs);

14.20. Possibilitar investigação forense remota, incluindo coleta de evidências e análise detalhada de eventos;

14.21. Suportar resposta automatizada a incidentes, como isolamento de dispositivo, bloqueio de processo e quarentena de arquivos;

14.22. Manter histórico completo dos eventos e respostas para auditoria e conformidade regulatória;

14.23. Permitir criação e customização de regras de detecção para adequação a diferentes ambientes;

14.24. Disponibilizar dashboards e relatórios detalhados sobre o status de segurança dos endpoints;

14.25. Integrar-se com sistemas SIEM e SOAR para automação e correlação de incidentes;

14.26. Oferecer suporte multiplataforma, incluindo Windows, macOS e Linux;

14.27. Identificar e bloquear comportamentos de ransomware em tempo real;

14.28. Alertar sobre acesso não autorizado a dados sensíveis ou sistemas críticos;

14.29. Possibilitar quarentena automático e manual de arquivos suspeitos;

14.30. Suportar integração com ferramentas de ticketing para gerenciamento eficiente de incidentes;

14.31. Deverá oferecer visibilidade completa dos processos ativos e conexões de rede nos endpoints;

Solução de Proteção e Prevenção de Vazamento de Dados (DLP)

14.32. Deverá permitir a análise contínua de dados associados a contas de usuário, identificando conteúdos sensíveis acessados, compartilhados ou modificados, tanto em dispositivos quanto em nuvem;

14.33. Deverá aplicar políticas de DLP (Data Loss Prevention) com base em identidade, considerando o comportamento histórico do usuário e o contexto da ação;

14.34. Deverá detectar e alertar sobre movimentações anômalas de dados feitas por contas com privilégios elevados, inclusive administradores de sistema e usuários com acesso a dados regulados;

14.35. Deverá integrar-se com Active Directory, Azure AD e Google Workspace, permitindo a sincronização automática de perfis, grupos e permissões;

14.36. Deverá identificar compartilhamento de arquivos sensíveis por usuários com terceiros, seja por e-mail, links públicos ou uploads não autorizados;

14.37. Deverá permitir respostas como revogação de permissões, bloqueio de conta, encerramento de sessão ou quarentena de dados manipulados;

14.38. Deverá possuir um dashboard com visão consolidada por usuário, destacando interações com dados sensíveis, dispositivos, apps conectados e volume de tráfego;

14.39. Deverá bloquear ou alertar sobre tentativas de upload de documentos confidenciais para domínios externos ou serviços não autorizados;

14.40. Deverá alertar sobre padrões suspeitos de login e movimentação de arquivos, incluindo logins simultâneos de locais distintos;

14.41. Deverá disponibilizar notificações via e-mail, webhook;

14.42. Deverá suportar integração com SIEMs para envio de incidentes correlacionados a identidade e exportação de score de risco por usuário;

Solução integrada de proteção avançada segurança cibernética Security Information&Event Management Threat Hunting

14.43. Esta seção detalha os requisitos técnicos para a contratação de uma solução de Security Information & Event Management (SIEM) e devera obrigatoriamente atender aos requisitos abaixo:

14.43.1. Requisitos de Infraestrutura:

14.43.1.1. Plataforma de SIEM em Nuvem Privada (SaaS) em Datacenter Tier3 localizado no Brasil, com possibilidade de integração, via API, com sistemas legados;

14.43.1.2. A solução deve ser capaz de coletar e processar dados de até 80 Devices (AD, FW e Servidores), com um volume de logs de até 300 GB/mês, e manter a retenção de dados por 30 dias;

14.43.1.3. Base de dados não compartilhada via Tenant, isto é, dedicada aos registros – Logs – para consulta;

14.43.1.4. Utilização de matriz MITRE ATT&CK.

14.43.2. Deverá suportar no mínimo os seguintes itens:

14.43.2.1. ARTIFICIAL INTELLIGENCE PROFILING;

14.43.2.2. Correlação de eventos;

14.43.2.3. Compliance com PCI-DSS, GDPR, LGPD e CCPA;

14.43.2.4. Agentes: Windows / Linux / MacOS 10.2.4.4.5 Docker / Kubernetes;

14.43.2.5. Perfil SIEM;

14.43.2.6. Análise de log do sistema;

14.43.2.7. Correlação de eventos de segurança;

14.43.2.8. Verificação de vulnerabilidade;

14.43.2.9. Monitoramento de integridade de arquivo;

14.43.2.10. Monitoramento de Políticas;

14.43.2.11. Relatório de Conformidade;

14.43.2.12. Monitoramento de segurança em nuvem;

14.43.2.13. Gestão de Ambiente;

14.43.2.14. Estrutura MITTRE ATTACK;

14.43.2.15. Cortex Threat Analytics;

14.43.2.16. Feed de inteligência de ameaças;

14.43.2.17. Mais de 100 regras de detecção de ameaças;

14.43.2.18. Detecção e resposta de endpoint;

14.43.2.19. Detecção e gerenciamento de ativos;

14.43.2.20. Resposta Automatizada a Incidentes.

14.43.3. Requisitos Operacionais e de Desempenho:

14.43.3.1. Escalabilidade: A arquitetura da solução deve ser escalável para acomodar o aumento futuro no volume de logs e no número de dispositivos monitorados, sem a necessidade de reestruturação;

14.43.3.2. Integração: A solução deve ser capaz de se integrar facilmente com as fontes de logs existentes no orgão, como os controladores de domínio (AD) e firewalls.

14.43.4. Requisitos de Funcionalidades Essenciais:

14.43.4.1. Gestão de Logs (Log Management):

14.43.4.1.1. A solução deve coletar logs de segurança de diversos dispositivos e sistemas, incluindo, mas não se limitando a sistemas operacionais (Windows, Linux), firewalls, servidores web e controladores de domínio (AD);

14.43.4.1.2. Deve normalizar e enriquecer os dados coletados, transformando-os em um formato padronizado para análise e correlação;

14.43.4.1.3. Realização de gerenciamento de registros diferentes fontes para identificar possíveis problemas de segurança integrada;

14.43.4.1.4. Detecção de intrusão: monitora e analisa o tráfego de rede em busca de sinais de possíveis ameaças à segurança, como malware ou acesso não autorizado;

14.43.4.1.5. Monitoramento de integridade de arquivos (FIM) com registros de alterações em arquivos e diretórios críticos do sistema para detectar modificações não autorizadas para fins de auditoria e investigação (incidentes de segurança);

14.43.5. Detecção de Intrusão (Intrusion Detection System – IDS):

14.43.5.1. A solução deve monitorar atividades maliciosas e tentativas de intrusão em tempo real, usando regras de detecção de ameaças pré-configuradas e personalizadas;

14.43.5.2. Deve ser capaz de detectar ataques de força bruta, atividade de malware e outras anomalias de rede;

14.43.5.3. Inteligência de ameaças com feeds de inteligência de ameaças para aprimorar os recursos de detecção contra ameaças conhecidas.

14.43.6. Monitoramento de Integridade de Arquivos (File Integrity Monitoring – FIM):

14.43.6.1. A solução deve monitorar continuamente a integridade de arquivos e diretórios críticos para o sistema, alertando sobre modificações, criações ou exclusões não autorizadas;

14.43.6.2. Deve ser possível definir quais arquivos e diretórios são críticos, com suporte para auditoria de eventos em tempo real;

14.43.7. Análise de Vulnerabilidades (Vulnerability Detection):

14.43.7.1. A solução deve realizar a varredura e a identificação de vulnerabilidades de segurança nos sistemas operacionais e aplicações instaladas nos servidores, gerando relatórios de risco;

14.43.7.2. Detecção de vulnerabilidades por agente instalado para varredura e análise de configurações e versões de software, com as integrações;

14.43.7.3. Elastic Stack (ELK Stack com o Elasticsearch, Logstash e Kibana (ELK Stack) para análise e visualização avançada de dados de segurança;

14.43.7.4. Amazon Web Services (AWS) e Microsoft Azure para monitoramento e segurança de instâncias, serviços e recursos na AWS e Azure;

14.43.7.5. Docker e Kubernetes com o monitoramento e proteção de contêineres Docker e clusters Kubernetes;

14.43.7.6. Microsoft Windows Event Forwarding (WEF) com a coleta de logs de eventos do Windows para análise e monitoramento;

14.43.7.7. Vírus Total para consulta de ameaças presentes nos registros desta base de dados;

14.43.7.8. Syslog com plataformas que utilizam este protocolo;

14.43.7.9. Resposta a Incidentes (Incident Response).

14.43.8. A plataforma deve permitir a criação de regras de resposta automática a incidentes, como o bloqueio de endereços IP maliciosos, o encerramento de processos suspeitos e o envio de alertas para a equipe de segurança;

14.43.9. **Console de Gestão e Dashboard**:

14.43.9.1. A solução deve oferecer um console de gestão web centralizado, com dashboards visuais e personalizáveis para monitorar o status de segurança, visualizar eventos e gerenciar alertas de forma intuitiva;

14.43.9.2. Monitoramento de conformidade com vários padrões normativos, monitorando e emitindo relatórios sobre controles de segurança.

14.43.10. **Relatórios**:

14.43.10.1. A solução deverá ter nativamente os seguintes tipos de relatórios que deverão ser entregues mensalmente até o quinto dia útil do mês:

14.43.10.1.1. LGPD;

14.43.10.1.2. NIST;

14.43.10.1.3. PCI;

14.43.10.1.4. Compliance.

Solução de Plataforma de Avaliação de Maturidade de Segurança da Informação com foco específico na capacidade de prevenção, detecção, resposta

14.44. A solução apresentada deverá, obrigatoriamente, atender no mínimo a todos os requisitos técnicos e funcionais aqui listados, sendo desclassificadas as propostas que não contemplarem integralmente tais requisitos:

14.44.1. A Plataforma Única de Avaliação e Monitoramento de Maturidade em Segurança Cibernética é a aquisição de uma plataforma de software única, destinada à gestão de maturidade cibernética e corporativa, devendo também, em sua arquitetura, ser uma solução única, coesa e integral, não se tratando de um conjunto de sistemas distintos, ainda que integrados, de diferentes fabricantes;

14.44.2. Apesar de ser fornecida por um único fabricante, a plataforma deve operar de forma integrada com outras soluções já existentes no ambiente tecnológico da organização, especialmente aquelas voltadas à prevenção, detecção e resposta a incidentes de segurança. Essa integração deve permitir a correlação automática de eventos e indicadores de comprometimento (IoCs) oriundos de ferramentas como SIEM, EDR/XDR, antivírus corporativo, soluções de backup e recuperação, sistemas de gestão de vulnerabilidades, firewalls de próxima geração (NGFW) e plataformas de gerenciamento de identidades e acessos (IAM/IDM), de modo a alimentar a análise de maturidade com dados em tempo quase real e gerar recomendações acionáveis.

Especificação Técnica da Plataforma

14.45. A plataforma deverá rodar na modalidade de SaaS e ficar hospedada no ambiente da CONTRATADA, sem gerar custos de manutenção da mesma pela CONTRATANTE;

14.46. A plataforma deverá possuir licenciamento específicos para software de governança, maturidade e avaliação de segurança da informação, módulo de assessment e devices sendo disponibilizadas de acordo com a tabela de quantidades especificada neste termo de referência;

14.47. A plataforma deverá possuir controle de acessos, com níveis diferenciados para administrador;

14.48. A plataforma deverá ter os inventários dos ativos, assim como o apontamento dos Ativos Críticos ao Negócio ou Serviços a fim de manter a avaliação continuada de risco;

Arquitetura e Tecnologias

14.49. Front-end: a interface do usuário (UI) da plataforma deverá ser por meio de um SaaS, garantindo uma experiência de usuário (UX) moderna, responsiva, interativa e de alta performance;

14.50. Back-end: a plataforma deverá possuir API RESTful escalável, eficiente e de alto desempenho, capaz de suportar um grande volume de requisições e processamento de dados. A API deve ser bem documentada (Swagger) e seguir princípios de segurança como autenticação, validação de entradas e proteção contra vulnerabilidades comuns;

14.51. Banco de Dados: o banco de dados deverá ser projetado com alta performance, com índices adequados, procedures otimizadas e um esquema de banco de dados robusto que garanta a integridade e consistência dos dados;

14.52. Infraestrutura de Hospedagem: toda a infraestrutura da plataforma (front-end, back-end e banco de dados) deverá ser hospedada no modelo SaaS;

14.53. Requisitos de Infraestrutura e Desempenho SaaS:

14.53.1. Ambiente SaaS de alta performance no Brasil;

14.53.2. Redundância de Zonas de Disponibilidade (Availability Zones) para alta resiliência, devendo ser projetada para garantir alta disponibilidade, utilizando recursos como múltiplos nós e balanceamento de carga com opções de redundância geográfica e failover automático;

14.53.3. Armazenamento com criptografia AES-256;

14.53.4. Banco de Dados relacional, que suporte linguagem T-SQL, com segurança avançada, criptografia de dados em repouso e em trânsito e controle de acesso baseado em funções (RBAC);

14.53.5. SLA (Service Level Agreement): a solução deverá garantir um SLA de 99,96% de disponibilidade para a plataforma como um todo, conforme os SLAs oferecidos pelos serviços de cloud de mercado;

14.53.6. Escalabilidade: a plataforma deve ser escalável horizontal e verticalmente para acomodar o crescimento futuro do volume de dados e do número de usuários, utilizando os recursos de autoescalabilidade dos serviços de cloud.

Segurança da Infraestrutura

14.54. Serão implementadas as melhores práticas de segurança no modelo SaaS, incluindo:

14.54.1. Rede Virtual (VNet): isolamento da rede da aplicação e banco de dados;

14.54.2. Grupos de Segurança de Rede (NSG): controle de tráfego de entrada e saída;

14.54.3. Gerenciamento seguro de chaves, segredos e certificados;

14.54.4. Integração para autenticação e autorização;

14.54.5. Monitoramento de segurança para detecção de ameaças e auditoria;

14.54.6. Backups e restauração: configuração de políticas de backup e recuperação de desastres para banco de dados e aplicações;

14.54.7. Firewall: configuração de firewall para o banco de dados e aplicações, permitindo acesso apenas de IPs autorizados;

14.54.8. Gerenciamento simplificado: a utilização dos serviços gerenciados deve proporcionar um gerenciamento simplificado da infraestrutura, reduzindo a complexidade operacional.

Plataforma de Segurança Cibernética e Maturidade

14.55. A solução deverá prover uma plataforma de Segurança Cibernética com foco em risco corporativo e técnico, contemplando, no mínimo:

14.55.1. Governança de segurança da informação;

14.55.2. Privacidade de dados;

14.55.3. Tecnologias de segurança da informação;

14.55.4. Monitoramento de maturidade;

14.55.5. Conformidade com frameworks de mercado;

14.55.6. Apontamento de melhorias por meio de inteligência artificial e melhores práticas;

14.55.7. Integração com ferramentas de segurança da informação.

14.56. A solução deverá ser capaz de:

14.56.1. Avaliar dados oriundos de sistemas de correlação e monitoramento (por exemplo, SIEM) e proporcionar entendimento do ambiente tecnológico;

14.56.2. Atribuir níveis de maturidade de 1 a 5 utilizando o modelo CMMI;

14.56.3. Atribuir pontuação de risco de 0 (risco mínimo) a 10 (risco crítico);

14.56.4. Indicar percentuais de atingimento de frameworks reconhecidos, tais como NIST, CIS, ISO 27000, requisitos de Seguro Cibernético e exigências oriundas de auditorias.

14.57. A solução deverá permitir a avaliação do uso de tecnologias e ferramentas de segurança da informação ao longo de todo o ciclo de:

14.57.1. Governança;

14.57.2. Identidade;

14.57.3. Proteção;

14.57.4. Detecção de ameaças;

14.57.5. Resposta a incidentes;

14.57.6. Recuperação.

Controles Avaliados

14.58. A solução deverá contemplar um conjunto de controles (em número superior a 450), aplicáveis a ferramentas e processos, incluindo, no mínimo:

14.58.1. Estratégia de gerenciamento de risco;

14.58.2. Funções, responsabilidades e autoridades;

14.58.3. Políticas de Segurança da Informação e regras;

14.58.4. Supervisão e auditoria;

14.58.5. Gerenciamento de risco da cadeia de suprimentos de segurança cibernética;

14.58.6. Gerenciamento de ativos;

14.58.7. Avaliação de risco;

14.58.8. Melhoria continuada;

14.58.9. Gerenciamento de identidade, autenticação e controle de acesso;

14.58.10. Conscientização e treinamento;

14.58.11. Segurança de dados;

14.58.12. Segurança de plataforma;

14.58.13. Resiliência da infraestrutura de tecnologia;

14.58.14. Monitoramento contínuo;

14.58.15. Análise de eventos adversos;

14.58.16. Gerenciamento de incidentes;

14.58.17. Análise de incidentes;

14.58.18. Relatórios e comunicação de resposta a incidentes;

14.58.19. Mitigação de incidentes;

14.58.20. Recuperação de incidentes – execução do plano;

14.58.21. Comunicação de recuperação de incidentes.

Relatório Integrado de Riscos e Vulnerabilidades

14.59. A solução deverá apresentar relatório integrado com os resultados de riscos e vulnerabilidades oriundos de testes de invasão (pentest), contemplando, no mínimo:

14.59.1. Identificação dos achados técnicos;

14.59.2. Avaliação de impacto;

14.59.3. Classificação de riscos e vulnerabilidades identificadas;

14.59.4. Recomendações de mitigação priorizadas.

Avaliação de Processos, Recursos e Controles

14.60. A solução deverá avaliar o uso de processos, recursos tecnológicos, recursos humanos e controles de segurança da informação nos seguintes temas:

14.60.1. Inventário e controle de ativos de software;

14.60.2. Proteção de dados e configuração segura de ativos corporativos e software;

14.60.3. Gerenciamento de contas;

14.60.4. Gerenciamento de controle de acesso;

14.60.5. Gerenciamento contínuo de vulnerabilidades;

14.60.6. Gerenciamento de log de auditoria;

14.60.7. Proteções de e-mail e navegador da web;

14.60.8. Defesas contra malware;

14.60.9. Recuperação de dados;

14.60.10. Gerenciamento de infraestrutura de rede;

14.60.11. Monitoramento e defesa de rede;

14.60.12. Conscientização sobre segurança e treinamento de habilidades;

14.60.13. Gerenciamento de provedores de serviços;

14.60.14. Segurança de software de aplicativo;

14.60.15. Gerenciamento de resposta a incidentes;

14.60.16. Teste de penetração.

Funções e Visões do Relatório de Maturidade

14.61. O relatório e os resultados fornecidos pela solução deverão contemplar, no mínimo, as seguintes visões:

14.61.1. Visão corporativa: focada em impactos financeiros, legais e reputacionais associados a falhas de segurança;

14.61.2. Visão técnica: análise de vulnerabilidades, falhas em sistemas e ameaças em tempo real;

14.61.3. Visão de governança: nível de atingimento percentual dos itens, com base em regras de governança, identidade, proteção, detecção de ameaças, resposta a incidentes e recuperação.

14.62. A solução deverá:

14.62.1. Atribuir pontuação por conformidade quanto ao uso de tecnologias, aplicação de processos de controle, controles manuais, automatizados e auditados;

14.62.2. Medir percentualmente os controles e apontar planos de ação, bem como sugestões para uso de tecnologias, processos e serviços;

14.62.3. Classificar os níveis de maturidade com base no modelo CMMI, contemplando os cinco níveis: Inicial, Gerenciado, Definido, Quantitativamente Gerenciado e Otimizado;

14.62.4. Correlacionar os níveis de maturidade com NIST CSF v2, CIS Controls v8 e ISO 27000;

14.62.5. Destacar os controles suportados por soluções de monitoramento (por exemplo, SIEM), atrelados a domínios, controles e políticas de NIST, CIS, LGPD, FIM e GDPR;

14.62.6. Prover controle de auditoria de conformidade da aplicação de políticas e controles, de forma manual e automatizada.

Escopo Temático da Avaliação e Mapa de Maturidade

14.63. A avaliação, bem como o relatório, deverá conter identificação, entendimento de riscos, uso, mapa de maturidade, pontuação de emprego nos ambientes tecnológicos e sua correlação com a proteção da CONTRATANTE, abrangendo, no mínimo, os seguintes itens:

14.63.1. Privacy & GRC;

14.63.2. Governance / Risk;

14.63.3. Data Security;

14.63.4. Third Party Risk Management;

14.63.5. Brand Protection / Deep-Dark Web / Anti-fraud;

14.63.6. Maturity Monitoring;

14.63.7. Software Supply Chain;

14.63.8. ITSM – Security;

14.63.9. SIEM;

14.63.10. DLP Cloud;

14.63.11. DLP Agent;

14.63.12. Patch Management;

14.63.13. Vulnerability Management – IAST – Discovery;

14.63.14. Asset Management Manual;

14.63.15. Asset Management Automatic;

14.63.16. Threat Intelligence;

14.63.17. DAST;

14.63.18. SAST;

14.63.19. AppSec / AST / APISec;

14.63.20. AI Security;

14.63.21. IoT/OT Security;

14.63.22. NetFlow;

14.63.23. Honeypot;

14.63.24. Bastion Host;

14.63.25. Sandbox;

14.63.26. Access Management & Authentication;

14.63.27. Observability – IT;

14.63.28. Topologia / Documentação / Arquitetura;

14.63.29. Observability – Physical / Patrimonial;

14.63.30. API / WAF;

14.63.31. NFW WAF;

14.63.32. NFW – IPS – Active Mode;

14.63.33. NFW – IDS – Monitoring Mode;

14.63.34. ASB;

14.63.35. SASE;

14.63.36. Anti-DDoS;

14.63.37. DNS Security;

14.63.38. NDR (Network Detection and Response);

14.63.39. NAC;

14.63.40. ZTNA;

14.63.41. ZTNS;

14.63.42. Safe Password;

14.63.43. Identity;

14.63.44. XDR;

14.63.45. EDR;

14.63.46. Antivirus;

14.63.47. Encryption Endpoint;

14.63.48. Encryption Server;

14.63.49. Encryption Database;

14.63.50. Encryption Data Network (em trânsito);

14.63.51. Cloud Security (vulnerabilidades, container security, IA security, microservices);

14.63.52. VM Security;

14.63.53. VPN;

14.63.54. Data Safe and Dispose Tools;

14.63.55. Digital Certificate;

14.63.56. MDM – Software Management;

14.63.57. Federation;

14.63.58. GPO;

14.63.59. Phishing Test / Awareness Platform;

14.63.60. PAM;

14.63.61. IAM;

14.63.62. SOAR;

14.63.63. EDR Incident Response / Retention / Eradication;

14.63.64. XDR Incident Response / Retention / Eradication;

14.63.65. Zero Trust / VLAN / Segmentação;

14.63.66. CASB / SASE;

14.63.67. Cloud Security;

14.63.68. DDoS Protection and Response;

14.63.69. Backup – On Premise;

14.63.70. Backup – Cloud;

14.63.71. Disaster Recovery.

Avaliação de Riscos, Frameworks e Políticas

14.64. A solução deverá avaliar riscos com pontuação clara e intuitiva de 0 (risco mínimo) a 10 (risco crítico), com base em contexto de políticas de segurança da informação.

14.65. A solução deverá:

14.65.1. Apresentar percentuais de atingimento dos frameworks reconhecidos;

14.65.2. Disponibilizar relatórios detalhados indicando a porcentagem de conformidade atingida para cada framework, permitindo priorização de esforços onde houver lacunas;

14.65.3. Destacar os controles por políticas, apresentando, no mínimo, as seguintes políticas e planos:

14.65.3.1. Política de Segurança da Informação;

14.65.3.2. Plano Estratégico de Segurança da Informação;

14.65.3.3. Risk Management Framework;

14.65.3.4. Política de Fornecedores e Cadeia de Suprimentos;

14.65.3.5. Política de Privacidade de Dados;

14.65.3.6. Política de Governança de Tecnologia e Anticorrupção;

14.65.3.7. Política de Melhoria Continuada e Auditoria Interna e Externa;

14.65.3.8. Política de Gerenciamento de Ativos;

14.65.3.9. Política de Gerenciamento de Vulnerabilidades;

14.65.3.10. Política de Gerenciamento de Inteligência de Ameaças;

14.65.3.11. Processo de Gerenciamento de Mudanças;

14.65.3.12. Plano de Continuidade de Negócios;

14.65.3.13. Plano de Resposta a Incidentes Cibernéticos;

14.65.3.14. Plano de Resposta a Incidentes de Privacidade de Dados;

14.65.3.15. Política de Uso da Internet;

14.65.3.16. Política de Segurança Física;

14.65.3.17. Política de Gerenciamento de Acesso;

14.65.3.18. Política de Gerenciamento de Conscientização;

14.65.3.19. Política de Criptografia;

14.65.3.20. Política de Cópias de Segurança;

14.65.3.21. Política de Desenvolvimento Seguro;

14.65.3.22. Política de Gerenciamento e Proteção de Endpoint;

14.65.3.23. Política de Teletrabalho e BYOD;

14.65.3.24. Política de Gerenciamento de Software, Imagens, Padrões e Hardening;

14.65.3.25. Política de Infraestrutura e Cloud Segura;

14.65.3.26. Política de Monitoramento de Segurança;

14.65.3.27. Política de Incidente de Segurança da Informação;

14.65.3.28. Política de Testes e Simulações de Ataques (Pen-test);

14.65.3.29. Política de Problemas de Segurança da Informação.

Controles Mínimos por Política e Auditoria

14.66. A solução deverá possuir controles de auditoria e maturidade realizados por especialistas, com validação das políticas atuais e indicação de possibilidade de utilização e melhoria;

14.67. Os relatórios providos pela plataforma deverão:

14.67.1. Avaliar, por política e controle, os níveis de maturidade segundo CMMI, NIST, CIS, ISO 27k e requisitos de Seguro Cibernético;

14.67.2. Apresentar recomendações para cada lacuna ou item não atendido, consolidadas por nível de conformidade, servindo como instrumento formal de auditoria.

14.68. A solução deverá suportar a avaliação, por política, contemplando, no mínimo, os seguintes quantitativos de controles:

14.68.1. Política de Segurança da Informação: mínimo de 17 controles;

14.68.2. Plano Estratégico de Segurança da Informação: mínimo de 7 controles;

14.68.3. Risk Management Framework: mínimo de 10 controles;

14.68.4. Política de Fornecedores e Cadeia de Suprimentos: mínimo de 26 controles;

14.68.5. Política de Privacidade de Dados: mínimo de 10 controles;

14.68.6. Política de Governança de Tecnologia e Anticorrupção: mínimo de 7 controles;

14.68.7. Política de Melhoria Continuada e Auditoria Interna e Externa: mínimo de 16 controles;

14.68.8. Política de Gerenciamento de Ativos: mínimo de 31 controles;

14.68.9. Política de Gerenciamento de Vulnerabilidades: mínimo de 22 controles;

14.68.10. Política de Gerenciamento de Inteligência de Ameaças: mínimo de 11 controles;

14.68.11. Processo de Gerenciamento de Mudanças: mínimo de 7 controles;

14.68.12. Plano de Continuidade de Negócios: mínimo de 7 controles;

14.68.13. Plano de Resposta a Incidentes Cibernéticos: mínimo de 7 controles;

14.68.14. Plano de Resposta a Incidentes de Privacidade de Dados: mínimo de 7 controles;

14.68.15. Política de Uso da Internet: mínimo de 8 controles;

14.68.16. Política de Segurança Física: mínimo de 7 controles;

14.68.17. Política de Gerenciamento de Acesso: mínimo de 41 controles;

14.68.18. Política de Gerenciamento de Conscientização: mínimo de 13 controles;

14.68.19. Política de Criptografia: mínimo de 13 controles;

14.68.20. Política de Cópias de Segurança: mínimo de 12 controles;

14.68.21. Política de Desenvolvimento Seguro: mínimo de 22 controles;

14.68.22. Política de Gerenciamento e Proteção de Endpoint: mínimo de 23 controles;

14.68.23. Política de Teletrabalho e BYOD: mínimo de 10 controles;

14.68.24. Política de Gerenciamento de Software, Imagens, Padrões e Hardening: mínimo de 22 controles;

14.68.25. Política de Infraestrutura e Cloud Segura: mínimo de 35 controles;

14.68.26. Política de Monitoramento de Segurança: mínimo de 48 controles;

14.68.27. Política de Incidente de Segurança da Informação: mínimo de 32 controles;

14.68.28. Política de Testes e Simulações de Ataques (Pen-test): mínimo de 11 controles;

14.68.29. Política de Problemas de Segurança da Informação: mínimo de 12 controles.

Recebimento e Tratamento de Registros de Incidentes

14.69. A solução deverá permitir o recebimento automatizado de registros de incidentes, incluindo, no mínimo:

14.69.1. Incidentes de Segurança da Informação relacionados a malware (vírus);

14.69.2. Phishing ou e-mails maliciosos direcionados a usuários;

14.69.3. Eventos de comando e controle (C2) que indiquem ação direta de agente externo na máquina monitorada;

14.69.4. Identificação de varredura de rede por meio de software que analise elementos internos sem autorização;

14.69.5. Avaliação contínua de comprometimentos, identificando atividades maliciosas dentro do ambiente da organização, incluindo comunicações com infraestrutura maliciosa na internet;

14.69.6. Inteligência de ameaças em tempo real, identificando ameaças conhecidas e desconhecidas com base em rede global de sensores ou fontes equivalentes;

14.69.7. Análise de inteligência de ameaças contextual, correlacionando eventos de segurança com informações adicionais para compreensão da gravidade e relevância das ameaças;

14.69.8. Interface de usuário intuitiva e painéis de controle para visualização e análise eficiente das informações de ameaças;

14.69.9. Capacidade de detectar e alertar sobre atividades suspeitas assim que identificadas, permitindo respostas rápidas;

14.69.10. Avaliação de risco de segurança cibernética com pontuações de risco para priorização de esforços;

14.69.11. Monitoramento de dark web e infraestrutura maliciosa com base em indicadores de comprometimento (IOCs), identificando comunicações com infraestrutura maliciosa.

Inspeção e Monitoramento de tráfego DNS.

14.70. A solução deverá prover inspeção e monitoramento de tráfego DNS, em modelo de confiança zero, incluindo:

14.70.1. Monitoramento e registro de tráfego DNS para identificação de consultas incomuns, padrões suspeitos ou comunicações com domínios maliciosos;

14.70.2. Identificação e análise de consultas DNS para nomes de domínio associados a infraestrutura maliciosa, botnets, ataques de phishing ou outras ameaças;

14.70.3. Utilização de análise comportamental para identificação de comportamentos anômalos no tráfego DNS, como consultas massivas ou a domínios suspeitos;

14.70.4. Identificação de comunicações ou conexões estabelecidas com domínios ou endereços IP conhecidos por hospedar ameaças, malware ou atividades maliciosas;

14.70.5. Identificação de domínios de comando e controle (C&C), rastreando comunicações entre sistemas internos e domínios utilizados por malwares;

14.70.6. Utilização de coletores instalados em gateways de acesso;

14.70.7. Geração de alertas em tempo real quando forem detectadas consultas DNS suspeitas ou atividades que indiquem potenciais ameaças;

14.70.8. Correlação de dados de DNS com outros eventos de segurança (por exemplo, logs de firewall, sistemas de detecção de intrusão), para análise abrangente e identificação de padrões de ameaça.

Requisitos adicionais da Plataforma de Monitoramento

14.71. A solução deverá:

14.71.1. Utilizar base de dados dedicada, não compartilhada via ambiente multi-tenant, para armazenamento dos registros (logs) e consultas;

14.71.2. Utilizar a matriz MITRE ATT&CK como referência para classificação de táticas, técnicas e procedimentos (TTPs) relacionados a eventos de segurança;

14.71.3. Realizar o gerenciamento de registros oriundos de diferentes fontes, de forma integrada, para identificar possíveis problemas de segurança;

14.71.4. Realizar detecção de intrusão, monitorando e analisando tráfego de rede em busca de sinais de possíveis ameaças, como malware ou acesso não autorizado;

14.71.5. Realizar monitoramento de integridade de arquivos (FIM), registrando alterações em arquivos e diretórios críticos para detectar modificações não autorizadas, com fins de auditoria e investigação;

14.71.6. Realizar detecção de vulnerabilidades mediante agente instalado, com varredura e análise de configurações e versões de software.

Interações

14.72. A solução deverá possuir, no mínimo, integrações com:

14.72.1. Elastic Stack (Elasticsearch, Logstash e Kibana), para análise e visualização avançada de dados de segurança;

14.72.2. Amazon Web Services (AWS) e Microsoft Azure, para monitoramento e segurança de instâncias, serviços e recursos em nuvem;

14.72.3. Docker e Kubernetes, para monitoramento e proteção de contêineres Docker e clusters Kubernetes;

14.72.4. Microsoft Windows Event Forwarding (WEF), para coleta de logs de eventos do Windows;

14.72.5. VirusTotal, para consulta de ameaças presentes nos registros;

14.72.6. Plataformas que utilizem protocolo Syslog.

14.73. A solução deverá ainda:

14.73.1. Monitorar conformidade com padrões normativos diversos, emitindo relatórios sobre controles de segurança avaliados;

14.73.2. Consumir e utilizar feeds de inteligência de ameaças para aprimorar a detecção de ameaças conhecidas.

Relatórios da Solução

14.74. A solução deverá fornecer, no mínimo, os seguintes relatórios:

14.74.1. Consolidação de eventos de segurança da informação por classificação de risco e categoria;

14.74.2. Consolidação de eventos com base na matriz MITRE ATT&CK, incluindo histórico de eventos, táticas de ataque, técnicas, regras, identificadores (IDs) e contadores;

14.74.3. Consolidação de registros de ambientes de nuvem pública;

14.74.4. Relatórios de conformidade para LGPD, PCI-DSS, GDPR e HIPAA.

14.74.4.1. O relatório de LGPD deverá contemplar, obrigatoriamente:

14.74.4.1.1. Domínios, atividades e artigos da Lei Geral de Proteção de Dados;

14.74.4.1.2. Relação direta entre eventos e artigos da lei;

14.74.4.1.3. Consolidação de eventos, volume mensal e distribuição percentual por artigo da lei;

14.74.4.1.4. Tipos de alertas e relação explicativa com os artigos da LGPD;

14.74.4.1.5. Tabela com visão por agente de coleta ou fonte, descrição técnica, contador e artigo da LGPD;

14.74.4.1.6. Utilização dos domínios e artigos da LGPD em documento mensal, com descrição explicativa.

14.74.4.2. A estrutura de governança para LGPD apresentada deverá contemplar, no mínimo:

14.74.4.2.1. Inventário de dados pessoais;

14.74.4.2.2. Manutenção da política de privacidade e proteção de dados;

14.74.4.2.3. Gerenciamento de riscos de segurança da informação;

14.74.4.2.4. Gerenciamento de riscos de terceiros;

14.74.4.2.5. Atualização e manutenção dos avisos de privacidade;

14.74.4.2.6. Atendimento às solicitações e reclamações de titulares de dados;

14.74.4.2.7. Monitoramento de novas práticas operacionais;

14.74.4.2.8. Manutenção de programa de gerenciamento de violação de privacidade de dados.

14.74.4.3. O relatório de conformidade para Seguro Cibernético deverá contemplar, no mínimo:

14.74.4.3.1. Domínios e atividades necessários ao atendimento dos requisitos de seguro cibernético;

14.74.4.3.2. Relação direta entre níveis de maturidade e requisitos do seguro;

14.74.4.3.3. Consolidação da pontuação atual e da pontuação ideal para aquisição ou manutenção de seguro cibernético;

14.74.4.3.4. Tipos de alertas que suportem melhores práticas para manutenção ou uso de controles que reduzam riscos para o seguro cibernético.

14.74.4.4. A estrutura de governança para Seguro Cibernético deverá abordar, no mínimo:

14.74.4.4.1. Políticas de segurança e gestão de risco;

14.74.4.4.2. Proteção aos sistemas de informação;

14.74.4.4.3. Operações e segurança de rede;

14.74.4.4.4. Segurança física em datacenter;

14.74.4.4.5. Serviços terceirizados (outsourcing);

14.74.4.4.6. Proteção de dados pessoais.

Solução de backup em nuvem e recuperação de desastres (DR) focada em proteção e rápida recuperação

14.75. Deverá entregar solução integrada de backup em nuvem e recuperação de desastres (Disaster Recovery – DR), em modelo de serviço, para proteção das cargas de trabalho de tecnologia da informação do CONTRATANTE, incluindo ambientes locais (*on-premises*), nuvens públicas, nuvens privadas e serviços de colaboração, visando assegurar a integridade, a confidencialidade e a disponibilidade das informações institucionais;

14.76. A solução deverá contemplar funcionalidades avançadas de proteção de dados, automação de rotinas de backup, orquestração de recuperação de desastres, proteção contra ransomware, monitoramento e geração de relatórios, observando as melhores práticas de mercado em proteção de dados e ciberproteção;

14.77. Deverá garantir a realização de backups consistentes, regulares e automatizados de servidores físicos, máquinas virtuais, estações de trabalho críticas, bancos de dados, aplicações corporativas e serviços de colaboração em nuvem;

14.78. Deverá possibilitar a rápida restauração de dados, sistemas e serviços em caso de incidentes de segurança (inclusive ransomware), falhas de hardware, erros operacionais ou desastres naturais, com redução do tempo de recuperação (RTO) e da perda aceitável de dados (POR);

14.79. Deverá disponibilizar ambiente de recuperação de desastres em nuvem para execução temporária das cargas de trabalho críticas, garantindo a continuidade dos serviços públicos até a recomposição do ambiente principal;

14.80. Deverá implementar mecanismos específicos de proteção contra ransomware e outras ameaças, incluindo detecção comportamental, antimalware/antivírus integrados e proteção de backups imutáveis contra alterações e exclusões não autorizadas;

14.81. Deverá simplificar a gestão da proteção de dados por meio de console único de administração, com autenticação forte, trilha de auditoria e relatórios gerenciais e de conformidade, compatíveis com as exigências de órgãos de controle e normas de segurança da informação;

14.82. Deverá permitir a implementação de estratégia de continuidade de negócios flexível, viabilizando a recuperação de sistemas críticos em ambientes de nuvem distintos, incluindo nuvem da própria solução e nuvem pública Microsoft Azure, de acordo com requisitos de disponibilidade, criticidade e resiliência definidos pelo CONTRATANTE;

14.83. Deverá contemplar, no mínimo, a proteção dos seguintes tipos de workloads:

14.84. Servidores físicos localizados em datacenters do CONTRATANTE;

14.85. Máquinas virtuais executadas em hipervisores suportados (tais como VMware ESXi, Microsoft Hyper-V, KVM ou equivalentes);

14.86. Servidores e cargas de trabalho em nuvens públicas suportadas;

14.87. Estações de trabalho e notebooks considerados críticos pelo CONTRATANTE;

14.88. Serviços de colaboração e produtividade em nuvem, incluindo correio eletrônico, armazenamento de arquivos e ferramentas de colaboração;

14.89. Bancos de dados e aplicações corporativas essenciais à continuidade dos serviços prestados pelo CONTRATANTE;

14.90. A solução deverá permitir expansão de capacidade (armazenamento, número de workloads, largura de banda efetiva) durante a vigência contratual, sem interrupção dos serviços, mediante solicitação do CONTRATANTE;

14.91. A solução deverá operar em modelo multi-tenant ou equivalente, permitindo segmentação lógica por unidade organizacional, se necessário, com isolamento e segregação de dados e políticas;

14.92. A solução deverá atender aos seguintes requisitos técnicos:

14.92.1. Arquitetura Geral;

14.92.2. A solução deverá ser baseada em plataforma de proteção de dados em nuvem, com console de gestão centralizado acessível via navegador web, suportando autenticação multifator (MFA) e controle de acesso baseado em perfis (RBAC).

14.93. Deverá permitir diferentes cenários de armazenamento de backup:

14.93.1. Backup de ambientes *on-premises* para armazenamento em nuvem provido pela solução;

14.93.2. Backup de ambientes *on-premises* para armazenamento local (appliance ou repositório em disco), com cópia secundária (replicação) para nuvem;

14.93.3. Backup de workloads em nuvens públicas para repositório de backup em nuvem ou outro armazenamento compatível, quando tecnicamente aplicável;

14.93.4. Deverá suportar múltiplos sistemas operacionais e plataformas, incluindo, no mínimo: Windows, Linux e macOS, bem como workloads de aplicações corporativas amplamente utilizadas (por exemplo, servidores de e-mail, bancos de dados e serviços de diretório).

14.94. Funcionalidades de Backup:

14.94.1. Suporte a backup em nível de arquivo, em nível de disco, em nível de imagem de sistema e em nível de aplicação (*application-aware*), garantindo consistência transacional para bancos de dados e serviços críticos;

14.94.2. Suporte a backups completos, incrementais e diferenciais, com mecanismos de deduplicação e compressão para otimização do uso de armazenamento e da largura de banda;

14.94.3. Disponibilizar opção de proteção de dados contínua (CDP), por meio de agente que monitore alterações em tempo real em aplicações e dados críticos, permitindo RPOs próximos de zero entre backups agendados;

14.94.4. Permitir configuração de políticas de retenção flexíveis por tipo de workload, com múltiplos horizontes de retenção (curto, médio e longo prazo), observando requisitos legais e normativos aplicáveis;

14.94.5. Oferecer agendamento de rotinas de backup com granularidade diária, semanal, mensal e por janelas de horário, com possibilidade de execução em períodos de menor utilização para minimizar impacto no desempenho dos sistemas produtivos;

14.94.6. Assegurar criptografia dos dados em trânsito e em repouso, utilizando algoritmos criptográficos robustos, amplamente aceitos no mercado, com gestão segura de chaves;

14.94.7. Permitir backups imutáveis, por meio de configuração de períodos em que os conjuntos de backup não possam ser modificados, sobrescritos ou apagados, mesmo por administradores com altos privilégios, reforçando a proteção contra ransomware;

14.94.8. Disponibilizar interface de gerenciamento que permita:

14.94.8.1. Criação de perfis de políticas reutilizáveis;

14.94.8.2. Aplicação em massa de políticas a grupos de dispositivos ou workloads;

14.94.8.3. Visualização centralizada do estado de proteção (protegido, desatualizado, com falha);

14.94.8.4. Monitoramento e geração de relatórios sobre volume de dados, taxas de sucesso, falhas e tendências.

14.94.9. Proteção Específica contra Ransomware e Ameaças Cibernéticas;

14.94.10. A solução deverá incorporar mecanismos de antimalware e antivírus baseados em análise comportamental e inteligência de máquina, capazes de detectar e bloquear ameaças de dia zero e variantes de ransomware, protegendo dados, sistemas e repositórios de backup;

14.94.11. Deverá monitorar atividades suspeitas relacionadas à criptografia massiva de arquivos e outras ações típicas de ransomware, gerando alertas, bloqueando processos maliciosos e preservando cópias íntegras dos dados;

14.94.12. Deverá possuir mecanismos de auto-proteção do agente de backup, impedindo a desativação, desinstalação ou alteração não autorizada por malware ou usuários mal-intencionados;

14.94.13. Deverá possibilitar *rollback* de arquivos e sistemas afetados ao estado imediatamente anterior ao incidente detectado, preservando registros das ações executadas e dos itens restaurados.

14.95. Requisitos de Segurança e Conformidade:

14.95.1. Suporte a autenticação multifator (MFA) para acesso de perfis administrativos ao console de gestão;

14.95.2. Controle de acesso baseado em funções (RBAC), permitindo criação de perfis de administrador global, administrador de unidade, operador e auditor, com segregação de funções;

14.95.3. Registro detalhado (logs) de todas as operações relevantes, incluindo: criação e alteração de políticas, início e término de *jobs* de backup e restauração, alterações de

configuração, acessos administrativos, com data/hora, usuário e origem, bem como capacidade de exportar tais registros para sistemas de auditoria e SIEM;

14.95.4. A solução deverá estar alinhada às boas práticas de proteção de dados e segurança da informação reconhecidas internacionalmente, tais como aquelas constantes em normas ISO/IEC 27001 ou equivalentes, sem que seja necessária a apresentação de certificação específica, salvo exigência de cláusula própria;

REQUISITOS TÉCNICOS DA SOLUÇÃO DE RECUPERAÇÃO DE DESASTRES (DR)

14.96. Funcionalidades de DR em Nuvem:

14.96.1. Disponibilizar ambiente de recuperação em nuvem capaz de executar temporariamente as cargas de trabalho protegidas, mediante conversão automática dos backups de servidores físicos ou virtuais em máquinas virtuais executáveis na infraestrutura de DR;

14.96.2. Permitir a criação de *runbooks* ou planos de recuperação orquestrados, definindo ordem de inicialização de máquinas, dependências entre serviços, configurações de rede, testes de validação e critérios de sucesso, com possibilidade de reutilização e versionamento;

14.96.3. Suportar realização de testes de plano de DR (simulados) em ambiente isolado, sem impacto no ambiente de produção, com geração de relatórios contendo tempos de recuperação, falhas encontradas e recomendações de melhoria;

14.96.4. Possibilitar procedimentos de *failover* (ativação do ambiente de DR) e *failback* (retorno ao ambiente principal), com o mínimo de intervenção manual, preservando consistência dos dados, incluindo sincronização das alterações realizadas durante o período de operação em DR;

14.96.5. Permitir configuração de diferentes RPO e RTO por grupo de sistemas, de acordo com a criticidade definida pelo CONTRATANTE, com mecanismos de monitoramento de aderência a esses parâmetros.

14.97. Requisitos de Rede e Conectividade:

14.97.1. Suportar a criação de redes virtuais em nuvem para execução das cargas de trabalho em DR, permitindo configuração de endereçamento IP, regras de firewall, NAT e demais elementos necessários à conectividade com usuários e sistemas externos;

14.97.2. Possibilitar a criação de túneis criptografados entre o ambiente de DR e o ambiente *on-premises* do CONTRATANTE, garantindo comunicações seguras durante testes e eventos reais de DR.

14.98. Monitoramento, Alertas e Relatórios de DR:

14.98.1. Disponibilizar monitoramento em tempo quase real do estado de replicação e da prontidão para DR, com indicadores de atraso de replicação, falhas, inconsistências e capacidade disponível;

14.98.2. Enviar alertas configuráveis (por e-mail e canais adicionais que a solução suportar) em caso de falhas de replicação, risco de descumprimento de RPO/RTO, ou divergências relevantes entre o ambiente de produção e o ambiente de DR;

14.98.3. Gerar relatórios de testes de DR, contemplando data e hora, sistemas envolvidos, tempos de recuperação obtidos, falhas identificadas e recomendações de correção, para fins de auditoria e melhoria contínua;

14.98.4. A solução deverá disponibilizar mecanismos nativos de orquestração de recuperação de desastres, baseados em políticas e fluxos automatizados, permitindo transformar cópias de backup em ambientes de execução temporários sem necessidade de reconstrução manual ou uso de ferramentas adicionais;

14.98.5. A orquestração deverá permitir a definição de planos de recuperação reutilizáveis, versionados e auditáveis, contemplando:

14.98.5.1. ordem de inicialização de máquinas virtuais e serviços;

14.98.5.2. dependências entre aplicações e sistemas;

14.98.5.3. parametrização automática de rede, endereçamento IP, DNS e regras de acesso;

14.98.5.4. validações técnicas e funcionais pós-ativação.

14.98.6. A execução dos planos de DR deverá ocorrer de forma automatizada, com acionamento manual ou programado, minimizando a intervenção humana e reduzindo riscos operacionais em situações de contingência;

14.98.7. Execução de DR em Nuvem da Solução e em Nuvem Pública Microsoft Azure;

14.98.8. A solução deverá suportar a ativação de ambientes de recuperação de desastres tanto em infraestrutura de nuvem gerenciada pela própria solução quanto em nuvem pública homologada, incluindo a plataforma **Microsoft Azure;**

14.98.8.1. Deverá ser possível executar as cargas de trabalho protegidas no ambiente de DR por meio da conversão automática dos backups em máquinas virtuais compatíveis, tanto para nuvem própria da solução quanto para nuvem pública Azure, preservando configurações essenciais de sistema, disco e rede.

14.98.9. A solução deverá permitir que o CONTRATANTE selecione, por plano de recuperação ou por grupo de sistemas, o destino do DR (nuvem da solução ou nuvem pública Azure), de acordo com requisitos técnicos, estratégicos, regulatórios ou de continuidade de negócios;

14.98.10. O modelo de operação deverá possibilitar a utilização sob demanda dos recursos computacionais de DR (processamento, memória e rede), sendo estes consumidos apenas durante testes ou eventos reais de desastre, evitando a necessidade de ambientes de contingência permanentemente ativos;

14.98.11. Após o encerramento do evento de DR, a solução deverá suportar o processo de retorno controlado ao ambiente principal (failback), incluindo sincronização das alterações

realizadas durante o período de operação em contingência, independentemente de o DR ter sido executado em nuvem própria da solução ou em nuvem pública Azure.

14.98.12. Governança e Auditoria de DR.

14.98.12.1. A solução deverá fornecer visibilidade centralizada da prontidão para recuperação de desastres, abrangendo ambientes protegidos com possibilidade de DR tanto em nuvem própria quanto em nuvem pública Azure;

14.98.12.2. Todas as operações relacionadas a DR — incluindo testes, ativações, execuções em Azure, alterações de planos e eventos de failover e failback — deverão ser registradas em trilhas de auditoria detalhadas, com data, hora, usuário responsável e resultado da operação;

14.98.12.3. A solução deverá disponibilizar relatórios técnicos e executivos consolidados, permitindo análise de desempenho, aderência a RPO/RTO, histórico de testes e auditorias, sem dependência de ferramentas externas.

Serviço de Centro de Operações de Segurança (SOC) tem por objeto prover à CONTRATANTE um ambiente operacional dedicado à detecção, análise, resposta e melhoria contínua frente a incidentes de segurança cibernética, atuando de forma integrada às soluções de segurança já contratadas ou a contratar (SIEM, EDR, DLP, firewall, proteção de e-mail, nuvem, identidade, entre outras)

14.99. SOC deverá operar de forma integrada com as soluções de segurança da CONTRATANTE (por exemplo, SIEM, EDR, DLP, ferramentas de nuvem, firewalls, antivírus, sistemas de logs e outras), fornecendo visibilidade consolidada, respostas coordenadas a incidentes, relatórios de conformidade e suporte às decisões de gestão de risco;

14.100. O Serviço de SOC o fornecedor atuará em parceria com a equipe interna da CONTRATANTE, executando atividades operacionais, transferindo conhecimento e apoiando a evolução da maturidade de segurança;

14.101. O serviço deverá atender os seguintes itens:

14.101.1. Estabelecer um ponto centralizado de monitoramento e resposta a incidentes de segurança, integrando eventos de múltiplas fontes (endpoints, redes, servidores, nuvem, identidade, e-mail, aplicações);

14.101.2. Reduzir o tempo de detecção (MTTD) e o tempo de resposta (MTTR) a incidentes, com processos bem definidos e equipe especializada;

14.101.3. Aumentar a capacidade de prevenção por meio de inteligência de ameaças, hunting proativo e ajuste contínuo de regras e políticas;

14.101.4. Apoiar a CONTRATANTE na conformidade com normas e regulamentações (LGPD, normas do GSI/PR, INs, auditorias de TCE/TCU, ISO 27001, etc.);

14.101.5. Promover a transferência de conhecimento e o desenvolvimento da equipe interna, reduzindo progressivamente a dependência do fornecedor para atividades rotineiras.

Modelo de Operação e Regime de Atendimento.

14.102. O serviço de SOC será prestado, **no mínimo**, em regime de **8x5** (oito horas por dia, cinco dias por semana, em dias úteis) ou, **24x7** (vinte e quatro horas por dia, sete dias por semana), incluindo turnos de atendimento e/ou plantão de sobreaviso para incidentes de alta criticidade, conforme necessidade da CONTRATANTE, para monitoramento, análise e resposta a incidentes de segurança da informação;

14.102.1. Regime 8x5 compreende a cobertura em horário comercial (08h às 18h e dias úteis), com plantão de sobreaviso para incidentes críticos fora desse período, se contratado;

14.102.2. Regime 24x7 compreende a cobertura ininterrupta (24 horas por dia, 7 dias por semana), com equipes em turnos, garantindo monitoramento, detecção e resposta contínuos.

14.103. O SOC deverá operar com equipe estruturada em **níveis de atendimento (N1, N2 e N3)**, com funções de:

14.103.1. Monitoramento e Triagem (Nível 1):

14.103.1.1. Monitorar continuamente (8x5 ou 24x7) os eventos e alertas gerados pelas fontes integradas, especialmente o SIEM;

14.103.1.2. Realizar triagem inicial (triagem) dos alertas, classificando criticidade e descartando falsos positivos;

14.103.1.3. Registrar todos os alertas relevantes em sistema de ITSM/Service Desk (quando a CONTRATNTE disponibilizar);

14.103.1.4. Escalar incidentes para análise aprofundada (Nível 2) conforme severidade e procedimentos definidos.

14.103.2. Análise e Investigação (Nível 2):

14.103.2.1. Analisar incidentes escalados, correlacionando eventos de múltiplas fontes;

14.103.2.2. Reconstruir a linha do tempo do incidente (timeline), identificar vetor de ataque, escopo e impacto;

14.103.2.3. Propor e, quando autorizado, executar ações de contenção e erradicação (isolamento de hosts, bloqueio de IPs/domínios, revogação de credenciais, quarentena de arquivos, etc);

14.103.2.4. Documentar achados e recomendações em relatório de incidente.

14.103.3. Resposta a Incidentes (Nível 3):

14.103.3.1. Coordenar a resposta a incidentes críticos, acionando equipes internas da CONTRATANTE e terceiros conforme plano de resposta;

14.103.3.2. Apoiar a execução de planos de recuperação (restauração de backups, failover, reconstrução de sistemas);

14.103.3.3. Conduzir análises pós-incidente (post-mortem), produzindo relatório de lições aprendidas e recomendações de melhoria.

14.103.4. Threat Hunting:

14.103.4.1. Planejar e executar campanhas regulares de Threat Hunting (ex.: mensais), baseadas em hipóteses de ataque, inteligência de ameaças e anomalias detectadas;

14.103.4.2. Utilizar o SIEM e demais ferramentas para buscar proativamente indicadores de comprometimento (IOCs) e táticas, técnicas e procedimentos (TTPs) de atores de ameaça;

14.103.4.3. Documentar os hunts realizados, achados e recomendações de melhoria em regras e políticas.

14.103.5. Gestão de Casos de Uso e Regras de Detecção:

14.103.5.1. Projetar, implementar e manter casos de uso de detecção no SIEM, alinhados ao perfil de risco da CONTRATANTE;

14.103.5.2. Revisar periodicamente regras de correlação, thresholds e listas de exceção para reduzir falsos positivos e melhorar a cobertura;

14.103.5.3. Incorporar inteligência de ameaças (feeds de IOCs, TTPs, relatórios de CTI) nas regras de detecção.

14.103.6. Inteligência de Ameaças (CTI):

14.103.6.1. Consumir e operacionalizar fontes de inteligência de ameaças (abertas, comerciais, governamentais, setoriais);

14.103.6.2. Produzir boletins e alertas de inteligência para a CONTRATANTE sobre ameaças relevantes ao seu setor e ambiente;

14.103.6.3. Apoiar a priorização de vulnerabilidades e ações de defesa com base em inteligência de ameaças.

14.103.7. Relatórios e Dashboards:

14.103.7.1. Produzir relatórios periódicos (diário/semanal/mensal) com Incidentes detectados e tratados; Tempo médio de detecção e resposta; Tendências de ameaças; Cobertura de casos de uso e Recomendações de melhoria;

14.103.7.2. Manter dashboards em tempo real para diferentes públicos (técnico, gestor, executivo).

Escopo Funcional do SOC – Atividades Operacionais.

14.104. O SOC deverá ser capaz de executar, **no mínimo**, as seguintes atividades, integrando o conjunto de itens listados tais como:

14.104.1. Avaliação dos eventos correlacionados;

14.104.1.1. Correlação de eventos de múltiplas fontes (rede, endpoint, nuvem, identidade, aplicações) com uso de plataforma de SIEM ou equivalente.

14.104.2. Suporte 8x5 ou 24x7 – Monitoramento;

14.104.2.1. Monitoramento contínuo, dentro do regime contratado, dos eventos de segurança e alertas relevantes.

14.104.3. Análise de log do sistema;

14.104.3.1. Coleta, normalização e análise de logs de sistemas operacionais, aplicações, dispositivos de rede, segurança e serviços em nuvem.

14.104.4. Verificação de vulnerabilidade;

14.104.4.1. Apoio à identificação e análise de vulnerabilidades, correlacionando achados com ativos e riscos para priorização de remediação.

14.104.5. Monitoramento de integridade de arquivo;

14.104.5.1. Acompanhamento de alterações em arquivos sensíveis ou críticos, conforme as capacidades das ferramentas disponíveis.

14.104.6. Monitoramento de Políticas;

14.104.6.1. Verificação da aplicação e conformidade de políticas de segurança, acesso, configuração e uso de recursos.

14.104.7. Relatório de Conformidade;

14.104.7.1. Elaboração de relatórios que demonstrem a aderência a políticas internas, normativos e frameworks de segurança.

14.104.8. Detecção e resposta de Endpoint;

14.104.8.1. Integração com soluções de EDR/antivírus, acompanhando alertas, apoiando a resposta e a remediação em endpoints.

14.104.9. Detecção e gerenciamento de ativos;

14.104.9.1. Identificação e monitoramento de ativos de informação e infraestrutura, dando suporte à gestão de inventário.

14.104.10. Resposta Automatizada a Incidentes;

14.104.10.1. Definição, configuração e operação de ações automatizadas de resposta (playbooks);

14.104.10.2. Deverá ter pelo menos uma lista de 100 playbooks já definidos.

14.104.11. Manutenção de Regras de Firewall e demais ferramentas;

14.104.11.1. Apoio à revisão e manutenção de regras de firewall, proxies e outras soluções de segurança, conforme fluxos acordados com a CONTRATANTE.

14.104.12. Suporte a auditorias;

14.104.12.1. Fornecimento de informações, relatórios e evidências para auditorias internas e externas, incluindo órgãos de controle.

14.104.13. Revisão de regras de segurança;

14.104.13.1. Revisão periódica de regras de segurança (SIEM, firewall, DLP, EDR, etc.), com base em incidentes, ameaças e recomendações de boas práticas.

14.104.14. Manutenção do Antivírus com identificação de vírus, ações de limpeza e atualização de segurança;

14.104.14.1. Acompanhamento e suporte na operação da solução antivírus, incluindo detecção, contenção e remediação.

14.104.15. Avaliação de Riscos.

14.104.15.1. Apoio à avaliação de riscos de segurança da informação, correlacionando eventos, vulnerabilidades e exposição de ativos.

Relatórios e Produtos de Informação do SOC.

14.105. O SOC deverá produzir relatórios e consolidações de informação, **no mínimo mensais**, contemplando todos os itens da seção, incluindo:

14.105.1. Consolidação de eventos por classificação de risco e categoria;

14.105.2. **Consolidação de eventos baseada no MITRE ATT&CK**, incluindo histórico de eventos, táticas de ataque, técnicas, regras, IDs e contadores;

14.105.3. **Consolidação dos registros de nuvem pública** – logs de ambientes IaaS, PaaS e SaaS utilizados pela CONTRATANTE;

14.105.4. **Relatórios de conformidade** para LGPD, NIST-800-53, PCI-DSS, GDPR e HIPAA (10.1.3.5), com evidências de controles e aderência a requisitos aplicáveis;

14.105.5. **Relatório específico de LGPD**, devendo, obrigatoriamente, contemplar:

14.105.5.1. Domínios, atividades e artigos da Lei;

14.105.5.2. Relação direta com eventos de segurança;

14.105.5.3. Consolidação de eventos, volume mensal e distribuição percentual por artigo da LGPD;

14.105.5.4. Tipos de alertas e relação explicativa com os artigos da LGPD;

14.105.5.5. Tabela proporcional com visão por agente de coleta ou fonte, descrição técnica, contador e artigo da LGPD;

14.105.5.6. Destaque mensal dos domínios e artigos da LGPD, com descrição explicativa.

14.105.6. Relatórios mensais com a Estrutura de Controle de Risco, incluindo:

14.105.6.1. Classificação de risco de acordo com o evento e sua classificação.

14.105.7. Relatórios de classes de controle NIST 800-53 e TSC, abrangendo:

14.105.7.1. Gerenciamento de controle de acesso;

14.105.7.2. Controle de privilégio mínimo;

14.105.7.3. Acesso aos sistemas controlados por logon;

14.105.7.4. Registros de acessos aos sistemas;

14.105.7.5. Auditoria de controles de acesso por meio de registros;

14.105.7.6. Identificação de falhas;

14.105.7.7. Proteção contra código não autorizado e malicioso;

14.105.7.8. Controles de acesso lógico e físico;

14.105.7.9. Identificação e controle do inventário de ativos de informação;

14.105.7.10. Conformidade com regras, políticas e procedimentos.

14.105.8. Estrutura de governança em segurança da informação e privacidade, com relatórios sobre:

14.105.8.1. Inventário de dados pessoais;

14.105.8.2. Manutenção da política de privacidade e proteção de dados;

14.105.8.3. Gerenciamento de riscos de segurança da informação e privacidade;

14.105.8.4. Gerenciamento de riscos de terceiros;

14.105.8.5. Atualização e manutenção de avisos;

14.105.8.6. Monitoramento de novas práticas operacionais;

14.105.8.7. Manutenção do programa de gerenciamento de violação de privacidade de dados.

14.105.9. Relatório de Conformidade para seguro cibernético, contemplando:

14.105.9.1. Domínios e atividades vinculadas aos requisitos de um seguro cibernético;

14.105.9.2. Relação direta com níveis de maturidade;

14.105.9.3. Consolidação da pontuação atual e da pontuação ideal para aquisição de seguro cibernético;

14.105.9.4. Tipos de alertas que evidenciem melhores práticas e controles para redução de risco.

14.105.10. Tipos de alertas que corroborem melhores práticas para a manutenção ou uso de controle para diminuição de riscos de um seguro cibernético.

Requisitos Técnicos, Operacionais e de Integração

14.106. A solução SOC deverá utilizar plataforma de correlação e gestão de eventos de segurança (SIEM ou equivalente) capaz de:

14.106.1. Integrar-se com as principais fontes de log da CONTRATANTE;

14.106.2. Suportar modelagem de casos de uso baseados em **MITRE ATT&CK;**

14.106.3. Gerar os relatórios de conformidade e governança.

14.107. Integração com SIEM**:**

14.107.1. O SOC deverá ser capaz de se integrar ao SIEM da CONTRATANTE (existente ou a ser implantado), consumindo eventos, alertas e dashboards;

14.107.2. Caso a CONTRATANTE ainda não possua SIEM, o fornecedor deverá:

14.107.2.1. Apoiar a especificação e implantação da solução de SIEM;

14.107.2.2. Operar o SIEM como parte do serviço de SOC, até que haja transferência para a CONTRATANTE, se desejado.

14.107.3. A integração deverá contemplar, no mínimo:

14.107.3.1. Fontes de log prioritárias (firewalls, proxies, EDR, DLP, AD/LDAP, e-mail, nuvem, servidores críticos);

14.107.3.2. Normalização e enriquecimento de eventos;

14.107.3.3. Configuração de casos de uso de detecção;

14.107.3.4. Dashboards e relatórios.

14.107.4. O SOC deverá integrar-se a um **sistema de ITSM/Service Desk** para registro, acompanhamento e histórico de incidentes, problemas e mudanças;

14.107.5. Deverá haver conectividade segura entre o SOC e o ambiente da CONTRATANTE (VPN, link dedicado ou mecanismo equivalente), em conformidade com a Política de Segurança da Informação da CONTRATANTE;

14.107.6. Os dados de logs e eventos permanecerão sob **titularidade da CONTRATANTE**, devendo o armazenamento, acesso e descarte obedecer às normas internas, à LGPD e às melhores práticas de segurança;

14.107.7. Requisitos de Governança, SLAs e Indicadores:

14.107.7.1. Deverão ser estabelecidos Acordos de Nível de Serviço (SLAs) para:

14.107.7.1.1. Tempo de acolhimento, classificação e resposta a incidentes, por severidade;

14.107.7.1.2. Disponibilidade do serviço SOC no regime contratual;

14.107.7.1.3. Prazo de entrega dos relatórios mensais.

14.107.8. O SOC deverá manter **rotina de governança**, contemplando:

14.107.8.1. Reuniões operacionais (quinzenais) para revisão de incidentes, ajustes de regras e planos de ação;

14.107.8.2. Reuniões executivas mensais para apresentação dos relatórios, indicadores de desempenho, riscos e recomendações.

14.107.9. Devera monitorar, entre outros, os seguintes indicadores mínimos:

14.107.9.1. Tempo médio de detecção (MTTD) e de resposta (MTTR) a incidentes;

14.107.9.2. Taxa de falsos positivos;

14.107.9.3. Percentual de incidentes tratados dentro dos SLAs;

14.107.9.4. Evolução da classificação de riscos e da maturidade em segurança.

14.107.10. **SLAs de atendimento conforme severidade**:

14.107.10.1. Crítico;

14.107.10.1.1. Tempo de Acolhimento ≤ 15 min (24x7) ou ≤ 30 min (8x5);

14.107.10.1.2. Tempo de Classificação ≤ 30 min;

14.107.10.1.3. Tempo de Resposta ≤ 1 hora.

14.107.10.2. Alto;

14.107.10.2.1. Tempo de Acolhimento ≤ 30 min;

14.107.10.2.2. Tempo de Classificação ≤ 1 hora;

14.107.10.2.3. Tempo de Resposta ≤ 4 horas;

14.107.10.3. Médio;

14.107.10.3.1. Tempo de Acolhimento ≤ 2 horas;

14.107.10.3.2. Tempo de Classificação ≤ 4 horas;

14.107.10.3.3. Tempo de Resposta ≤ 12 horas;

14.107.10.4. Baixo.

14.107.10.4.1. Tempo de Acolhimento ≤ 8 horas;

14.107.10.4.2. Tempo de Classificação ≤ 24 horas;

14.107.10.4.3. Tempo de Resposta conforme planejamento.

14.107.11. Realizar reuniões de governança:

14.107.11.1. Reunião tática semanal para análise de tendências e ajustes;

14.107.11.2. Reunião executiva mensal para apresentação de resultados, KPIs e plano de ação.

14.107.12. Restrições e Conformidade Legal:

14.107.12.1. A atuação do SOC deverá estar estritamente alinhada à **Política de Segurança da Informação e Proteção de Dados** da CONTRATANTE, bem como à **LGPD** e demais normas internas e externas aplicáveis;

14.107.12.2. A CONTRATADA deverá garantir que todo o atendimento, documentação e comunicação sejam realizados em **língua portuguesa (PT-BR);**

14.107.12.3. O SOC deverá manter registro e trilha de auditoria de todas as ações executadas em nome da CONTRATANTE, permitindo a rastreabilidade para fins de auditoria interna, externa e de controle.

14.107.13. Equipe do SOC:

14.107.14. O fornecedor deverá disponibilizar equipe dimensionada conforme o regime contratado (8x5 ou 24x7), com no mínimo:

14.107.14.1. Quantidade mínima (8x5);

14.107.14.1.1. **01** Gerente do SOC - Profissional sênior, responsável pela gestão do serviço, governança e interface com a CONTRATANTE;

14.107.14.1.2. **01** Analista Líder / Especialista SIEM & Hunting - Profissional sênior, responsável por casos de uso, hunting e análises complexas;

14.107.14.1.3. **01** Analista de Segurança Nível 2 - Profissional pleno/sênior, responsável por investigação e resposta;

14.107.14.1.4. **01** Analista de Segurança Nível 1 - Profissional júnior/pleno, responsável por monitoramento e triagem.

14.107.14.2. Quantidade mínima (24x7).

14.107.14.2.1. **01** Gerente do SOC - Profissional sênior, responsável pela gestão do serviço, governança e interface com a CONTRATANTE;

14.107.14.2.2. **01** Analista Líder / Especialista SIEM & Hunting - Profissional sênior, responsável por casos de uso, hunting e análises complexas;

14.107.14.2.3. **02** Analista de Segurança Nível 2 - Profissional pleno/sênior, responsável por investigação e resposta;

14.107.14.2.4. **04** Analista de Segurança Nível 1 - Profissional júnior/pleno, responsável por monitoramento e triagem.

Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM)

14.108. Gerenciamento de Endpoints:

14.108.1. Solução de Gerenciamento Unificado de Endpoints baseada em plataforma de RMM em nuvem com agente único, que integra funcionalidades de gestão e segurança: patching, inventário, distribuição de software, controle de vulnerabilidades, backup e recuperação a partir de um único console centralizado e seguro;

14.108.2. Simplificar a gestão da proteção de dados, da continuidade de negócios e da operação dos ambientes de TI por meio de console único de administração, integrando funcionalidades de backup, recuperação de desastres, monitoramento contínuo, automação operacional e segurança, com controle de acesso, auditoria e relatórios gerenciais.

14.109. Requisitos Gerais:

14.109.1. A solução deve suportar a aplicação de patches para diversos sistemas operacionais (Windows, Linux e macOS), incluindo desktops, laptops e servidores, de forma centralizada, utilizando uma única interface de gerenciamento baseada em console web;

14.109.2. A solução deve suportar usuários conectados via VPN, redes corporativas e usuários com acesso direto à internet, permitindo o gerenciamento remoto mesmo fora da rede da empresa;

14.109.3. A solução deve operar sem exigir que os computadores pertençam a um domínio ou serviço de diretório, devendo, entretanto, ser capaz de se integrar a uma ou mais estruturas de diretório (como AD, Azure AD) para descoberta e agrupamento lógico de dispositivos, quando presentes;

14.109.4. A aplicação de patches e demais tarefas de gestão para todos os locais remotos devem ser orquestrada centralmente pelo console de gerenciamento da solução em nuvem, com uso de agentes e, quando aplicável, proxies de rede ou componentes intermediários recomendados pelo fabricante;

14.109.5. A solução deve funcionar adequadamente em conexões de baixa velocidade em locais remotos, otimizando o tráfego e permitindo agendamento de atividades fora do horário de pico;

14.109.6. A solução deve auxiliar na limitação da largura de banda consumida por tarefas de gestão (patches, distribuição de software, scripts, backup e outras), com perfis de throttling configuráveis, sem depender exclusivamente dos recursos nativos do sistema operacional;

14.109.7. Em caso de qualquer vulnerabilidade crítica de zero-day, a solução deve suportar a implementação rápida de medidas de mitigação e soluções alternativas de segurança recomendadas pelo fabricante da solução e pelos OEMs (por exemplo, scripts, políticas de bloqueio, regras de NGAV), em toda a empresa;

14.109.8. A solução deve manter o inventário de ativos de hardware e software, com todas as informações disponíveis centralmente no console do cliente ou parceiro, com atualização automática a partir dos agentes;

14.109.9. A solução deve suportar a criação e implantação remota de imagens ou planos de provisionamento de sistemas operacionais Windows, integrando, quando aplicável, recursos de backup e restauração para acelerar o onboarding e recovery de endpoints;

14.109.10. A solução deve suportar a distribuição de software para Windows, macOS e Linux, utilizando agentes gerenciados e pontos de distribuição ou mecanismos de cache quando disponíveis;

14.109.11. A solução deve ser capaz de relatar proativamente as alterações nos desktops e servidores gerenciados, de forma periódica ou em tempo quase real, após a detecção da alteração ou após a execução de qualquer ação implantada a partir do servidor (por exemplo, aplicação de patch, instalação de software, alteração de política);

14.109.12. A solução deve incluir um software agente único implantado em todos os dispositivos gerenciados, responsável por coleta de inventário, execução de políticas, tarefas de patching, backup, segurança e automações de RMM;

14.109.13. Se qualquer informação, patch, pacote de software ou carga útil for baixada da internet ou do repositório do fabricante, a integridade desse conteúdo deve ser verificada pela solução usando mecanismos de validação (como checksums, assinaturas digitais e conexões TLS) para garantir que o conteúdo baixado não tenha sido modificado ou corrompido;

14.109.14. A solução deve disponibilizar APIs RESTful totalmente documentadas para integração com outras ferramentas complementares, como ITSM, SIEM, PSA e plataformas de automação;

14.109.15. A solução deve fornecer políticas de gerenciamento de patches prontas para uso, alinhadas às melhores práticas e recomendações do fabricante, de forma que os administradores possam aplicar patches nas plataformas de sistema operacional suportadas, utilizando aplicação de patches e personalização baseadas em políticas e grupos de dispositivos.

14.110. Arquitetura**:**

14.110.1. A solução deve suportar um ambiente distribuído, incluindo sites em modelo hub-and-spoke conectados por diversos links de rede, variando de menos de 1 Mbps a 2 Mbps ou mais, mantendo a gestão centralizada em um console em nuvem ou servidor central;

14.110.2. A solução deve ser capaz de usar dispositivos clientes existentes como pontos de distribuição ou caches em locais remotos, quando suportado pelo fabricante, reduzindo a necessidade de servidores dedicados nesses locais;

14.110.3. A solução deve ter capacidade nativa de limitar a largura de banda usada para download e upload de atualizações, patches, pacotes de software, dados de telemetria e backup, com perfis de throttling estáticos ou dinâmicos para upstream e downstream entre servidores e agentes;

14.110.4. A solução deve suportar o armazenamento em cache de conteúdo (patches, pacotes, atualizações) em pontos de distribuição em escritórios remotos, sempre que essa funcionalidade estiver disponível na arquitetura recomendada pelo fabricante;

14.110.5. A solução deve ser capaz de baixar e armazenar em cache a carga útil nos pontos de distribuição remotos ou nos próprios agentes, antes do horário agendado para uma ação, de forma a otimizar o uso da rede no momento da execução;

14.110.6. A solução deve operar usando portas configuráveis para todas as comunicações entre agentes, pontos de distribuição, componentes on-premises (quando existirem) e o console em nuvem, respeitando as melhores práticas de segurança e documentação do fabricante;

14.110.7. A solução deve garantir a conformidade contínua, avaliando dispositivos fora da rede da empresa e gerenciando dispositivos em roaming, usando escopo de IP, identificadores de

agente e políticas de segurança que se apliquem tanto a dispositivos on-premises quanto remotos;

14.110.8. O agente deve permanecer leve e ocioso em termos de consumo de recursos até que tarefas sejam agendadas ou políticas exijam ação, mantendo, entretanto, comunicação periódica com o servidor para receber instruções, atualizações de políticas, assinaturas e metadados;

14.110.9. A solução deve ser compatível com Windows, Linux e macOS, com cobertura de agentes e funcionalidades de gestão, patching, inventário e segurança aderentes ao escopo definido pelo fabricante para cada sistema operacional;

14.110.10. A solução deve fornecer um utilitário de implantação remota de agentes que permita instalação remota em escala, podendo usar serviços de diretório, domínios, credenciais de administrador local ou pacotes instaladores distribuídos por outros meios (por exemplo, scripts, ferramentas de terceiros);

14.110.11. A estratégia de implantação de agentes deve considerar múltiplos métodos, incluindo políticas de grupo, scripts de login, distribuição via e-mail com link para instalador, ferramentas de distribuição de terceiros e instalação manual, de acordo com as orientações do fabricante;

14.110.12. A solução deve suportar procedimentos documentados para incluir o agente como parte de uma imagem padrão do sistema operacional ou de um processo automatizado de provisionamento de dispositivos;

14.110.13. A solução deve fornecer procedimentos de atualização in-place, centralizados e fáceis de usar para todos os componentes, agentes e módulos, por meio do console de gerenciamento, sem exigir reinstalações manuais;

14.110.14. A solução deve usar uma única interface de usuário de gerenciamento, baseada em console web, para todos os recursos, funções e componentes de RMM, backup e segurança;

14.110.15. A solução deve ter suporte nativo para comunicações criptografadas de alto nível (por exemplo, TLS 1.2 ou superior) entre agentes, componentes intermediários e console, sem necessidade de instalação de softwares de terceiros, certificados externos adicionais ou infraestrutura de autoridade certificadora própria, exceto se o cliente desejar integrá-la;

14.110.16. A solução deve incluir capacidade de alta disponibilidade e failover de acordo com o modelo de implantação escolhido (nuvem gerenciada pelo fabricante ou componentes on-premises), para atender a cenários como falha de hardware ou desastre no local, conforme melhores práticas;

14.110.17. Quando aplicável, a solução deve oferecer opções para operação em rede isolada (air-gap) ou ambientes com conectividade restrita, devendo ser possível sincronizar atualizações e políticas por meio de mecanismos seguros recomendados pelo fabricante;

14.110.18. A solução deve ser capaz de baixar e armazenar em cache cargas úteis (patches, pacotes, atualizações de agente) previamente à execução de ações agendadas, reduzindo o impacto em horários críticos de produção;

14.110.19. A solução deve garantir conformidade contínua avaliando dispositivos dentro e fora da rede da empresa, gerenciando dispositivos em roaming com base em agentes instalados, políticas e escopos lógicos de agrupamento.

14.111. Gerenciamento de Patches:

14.111.1. A solução deve fornecer avaliação de patches pronta para uso, com ciclos automáticos de varredura e correlação com metadados do fabricante, sem necessidade de agendamentos manuais complexos para verificação de patches ou inventário;

14.111.2. O agente deve relatar automaticamente, em intervalos configuráveis, o resultado da avaliação de patches assim que o servidor distribuir os novos metadados ou assinaturas de patch fornecidos pelo fabricante;

14.111.3. A solução deve utilizar métodos robustos para determinar se um patch foi instalado no cliente, como inspeção de registro, verificação de arquivos, checagem de número de versão e uso de métodos proprietários do OEM que aplica o patch;

14.111.4. A solução deve ser capaz de determinar dependências de patches antes da implantação, garantindo que pré-requisitos sejam atendidos nos endpoints;

14.111.5. A solução deve ser capaz de determinar se um patch já foi instalado em um endpoint e se um patch mais recente substitui versões anteriores, tratando o endpoint como atualizado quando for o caso;

14.111.6. A solução deve permitir o agrupamento manual e dinâmico de computadores com base em informações de ativos, sistema operacional, localização, funções e softwares instalados, facilitando políticas de patching segmentadas;

14.111.7. As descrições e os níveis de gravidade dos patches devem estar disponíveis na solução, incluindo, quando fornecido pelo fabricante ou OEM, hyperlinks para informações detalhadas dos patches nos sites dos fornecedores de software;

14.111.8. Os patches disponibilizados pela solução devem ser testados de acordo com as práticas padrão do fabricante, e a solução deve permitir que administradores configurem ambientes de teste/piloto e sejam notificados sobre eventuais problemas conhecidos;

14.111.9. A solução deve permitir que o operador do console implante patches em todos os computadores ou direcione computadores específicos para a implantação de patches a partir do console central, sem intervenção dos usuários finais;

14.111.10. A solução deve permitir que o operador defina diferentes políticas de implantação de patches (por exemplo, por grupo, criticidade, janela de manutenção) e crie políticas personalizadas;

14.111.11. A solução deve ser capaz de fornecer monitoramento em tempo quase real do status da implantação de patches, com visibilidade por dispositivo, grupo e nível de sucesso/erro;

14.111.12. A solução deve permitir que os operadores implantem vários patches simultaneamente, sempre que aplicável, minimizando reinicializações e consolidando reinícios quando necessários;

14.111.13. A solução deve permitir que os operadores distribuam a implantação de patches ao longo de um período predefinido, para reduzir o impacto geral na largura de banda da rede e em janelas de produção;

14.111.14. A solução deve permitir mensagens pop-up ou notificações personalizáveis para usuários antes da instalação de patches, e permitir que usuários com privilégios adequados adiem a instalação e a reinicialização dentro de limites definidos pelo operador do console;

14.111.15. A solução deve ter capacidade de reimplantar automaticamente patches em computadores onde a implantação inicial não foi bem-sucedida ou onde o patch tenha sido removido pelo usuário, conforme políticas definidas;

14.111.16. A solução deve suportar a aplicação de patches para uma variedade de aplicações padrão de diversos fornecedores (por exemplo, Microsoft, Google, Mozilla, Apple, Oracle e outros), conforme catálogo suportado pelo fabricante;

14.111.17. A solução deve ter capacidade de armazenar em cache patches nos diversos pontos de distribuição ou agentes designados, reduzindo o tráfego repetido na WAN;

14.111.18. A solução deve ter capacidade de instalar automaticamente patches previamente aprovados em computadores adicionados posteriormente à rede ou ao tenant, alinhando novos endpoints às políticas vigentes;

14.111.19. A solução deve ter capacidade de excluir automaticamente arquivos de instalação de patches do disco rígido dos computadores assim que a instalação for concluída com sucesso, otimizando o uso de armazenamento;

14.111.20. O administrador deve ser capaz de direcionar patches específicos para todas as máquinas com propriedades definidas (por exemplo, função, versão de SO, localização, tags ou grupos);

14.111.21. O sistema deve ser capaz de verificar a relevância do patch para cada endpoint antes de implantá-lo, evitando instalações desnecessárias;

14.111.22. A solução deve suportar a implantação de patches fora do período de suporte do fabricante (quando tecnicamente possível) ou a criação de políticas específicas para lidar com sistemas em fim de vida (EOL);

14.111.23. A solução deve identificar o fim da vida útil (EOL) de sistemas operacionais Windows e outros, entre os dispositivos gerenciados, permitindo relatórios e ações de mitigação;

14.111.24. A solução deve fornecer a opção de executar ações prévias, como desligar bancos de dados ou serviços específicos, antes da implantação de patches, com capacidade de executar ações pós-implantação, conforme necessário;

14.111.25. A solução deve identificar computadores que necessitam de rollback de patch (quando suportado) e permitir aos operadores monitorar o processo e relatar se o rollback foi bem-sucedido.

14.112. Inventário de Hardware e Software:

14.112.1. A solução deve recuperar automaticamente informações de inventário de hardware dos sistemas com agentes instalados, sem dependência de varreduras manuais agendadas;

14.112.2. As alterações de inventário devem ser processadas automaticamente pelo agente e enviadas periodicamente ao servidor, sem intervenção do operador;

14.112.3. Todas as informações sobre ativos de hardware devem ser registradas no servidor de gerenciamento, incluindo, no mínimo: velocidade e tipo da CPU, memória, espaço em disco rígido, nome do computador, modelo, endereço IP, sistema operacional e periféricos conectados, conforme capacidades do agente;

14.112.4. A solução deve listar todos os softwares e aplicações instalados, incluindo números de versão e serviços em execução associados, permitindo visibilidade do portfólio de aplicações por endpoint;

14.112.5. A solução deve permitir que operadores do console criem consultas personalizadas sobre as informações de hardware e software e agrupem computadores dinamicamente com base nessas propriedades, para fins de gestão, patching e conformidade;

14.112.6. A solução deve permitir que operadores realizem ações remotas baseadas em inventário, como executar scripts, coletar informações adicionais ou iniciar tarefas em um conjunto de máquinas selecionadas;

14.112.7. A interface web deve permitir acesso baseado em funções (RBAC) para conceder ou restringir privilégios dos usuários administradores, bem como oferecer recursos de visualização, filtragem e classificação para criação de relatórios.

14.113. Distribuição de Software e Implantação de SO:

14.113.1. A solução deve suportar a implantação de múltiplos formatos de pacotes, incluindo EXE, MSI e outros formatos equivalentes compatíveis com os sistemas operacionais suportados;

14.113.2. A solução deve permitir que operadores distribuam softwares de terceiros ou internos para computadores específicos, grupos de dispositivos ou tenants completos;

14.113.3. A solução deve fornecer abordagem assistida por assistente (wizard) para configurar informações do pacote, definir critérios de aplicabilidade e parâmetros de instalação silenciosa ou interativa;

14.113.4. A solução deve oferecer, quando aplicável, um portal de autosserviço ou mecanismo semelhante que permita ao usuário final instalar pacotes de software pré-aprovados atribuídos ao dispositivo ou usuário;

14.113.5. A solução deve permitir que operadores especifiquem critérios de sucesso da implantação de software (códigos de retorno, presença de arquivos, versão instalada, entre outros);

14.113.6. A solução deve ser capaz de suportar a criação de imagens, planos de provisionamento ou fluxos de implantação de sistemas operacionais, bem como integrar-se a recursos de backup para preservar e restaurar perfis de usuário em máquinas de destino, quando suportado;

14.113.7. A solução deve ser capaz de criar vários modelos de implantação e suportar atividades pós-implantação, como alteração de nome do computador, associação a domínios e OUs, criação de contas locais e de domínio, e restauração de dados e perfis de usuário;

14.113.8. A solução deve suportar a instalação de múltiplos drivers e aplicações durante o processo de pós-implantação, conforme pacotes definidos pelos administradores;

14.113.9. A solução deve suportar múltiplos meios de inicialização e implantação (por exemplo, PXE, USB, ISO ou métodos equivalentes suportados pelo fabricante);

14.113.10. A solução deve suportar escritórios remotos com pontos de distribuição ou mecanismos de cache para replicar imagens, pacotes e drivers com eficiência;

14.113.11. A solução deve ser capaz de realizar implantações com mínima ou nenhuma intervenção manual, incluindo implantação autônoma para usuários em home office, dentro das capacidades suportadas;

14.113.12. A solução deve suportar implantações baseadas em senha, seleção de modelo ou políticas, e ter gerenciamento de drivers que permita coleta de drivers de máquinas de referência e sua aplicação durante a implantação.

14.114. Controle Remoto:

14.114.1. O módulo de controle remoto deve permitir assumir o controle total de desktops e servidores a partir de um local central, utilizando o console da solução;

14.114.2. A solução deve suportar recursos de segurança para o controle de PCs remotos, baseados em políticas e autorizações predefinidas, com autenticação forte e registro de sessões;

14.114.3. A solução deve suportar criptografia robusta (por exemplo, AES-256) durante as operações de acesso remoto, garantindo confidencialidade do tráfego;

14.114.4. A solução deve proporcionar flexibilidade quanto ao tipo e capacidade da sessão de controle remoto: controle total, modo somente monitor, bloqueio de teclado e mouse, bate-papo interativo e transferência de arquivos, conforme recursos disponíveis no módulo de acesso remoto;

14.114.5. O módulo de controle remoto deve ser gerenciado por políticas centralizadas, permitindo que equipes de TI definam quem terá permissão para acessar quais alvos, de que forma e em quais horários;

14.114.6. Deve ser possível restringir o nível de operações que um administrador pode executar, diferenciando perfis como controle total, apenas monitoramento, reinicialização e transferência de arquivos;

14.114.7. Para maior proteção contra abuso, os usuários finais devem ser avisados sobre o início das sessões de controle remoto, podendo ser exigida a aceitação do usuário, com possibilidade de encerrar ou revogar o controle a qualquer momento, conforme políticas definidas;

14.114.8. O módulo de controle remoto deve ser capaz de criar listas ou grupos de destino para restringir o acesso de administradores a subconjuntos específicos de máquinas;

14.114.9. O controle remoto deve ser acessível via interface web autenticada, com log centralizado das sessões, autenticação integrada, criptografia de fluxo de dados, bloqueio automático por inatividade e, quando suportado, recursos de colaboração entre múltiplos operadores;

14.114.10. A solução deve suportar funcionalidades de Wake on LAN ou mecanismos equivalentes para ligar dispositivos remotamente, quando tecnicamente viável;

14.114.11. A solução deve permitir encerrar ou interromper processos em execução no dispositivo remoto, de forma controlada;

14.114.12. A solução deve permitir o envio de mensagens ou avisos simultâneos para um grande número de usuários ou computadores gerenciados;

14.114.13. A solução deve permitir gerenciar remotamente processos, serviços e softwares em endpoints sem exigir intervenção do usuário final, respeitando as permissões concedidas.

14.115. Políticas de Segurança e Configuração:

14.115.1. A solução deve ser capaz de identificar endpoints com aplicações ou agentes específicos e desinstalá-los ou substituí-los remotamente, quando suportado pelo sistema operacional e políticas de segurança;

14.115.2. A solução deve ser capaz de iniciar e parar serviços em máquinas remotas sem necessidade de interação do usuário, por meio de scripts ou comandos remotos;

14.115.3. A solução deve ser capaz de desligar ou reiniciar qualquer máquina gerenciada remotamente, seguindo janelas de manutenção e políticas de aprovação;

14.115.4. A solução deve ser capaz de distribuir e instalar certificados digitais em endpoints para aprimorar a segurança, incluindo certificados para autenticação, criptografia ou inspeção, de acordo com os requisitos do cliente;

14.115.5. A solução deve ser capaz de conceder e revogar permissões em arquivos, pastas e chaves de registro para usuários ou grupos, por meio de scripts ou políticas de configuração, compatíveis com os sistemas operacionais suportados;

14.115.6. A solução deve ser capaz de controlar propriedades de firewall de endpoint, definindo regras de firewall personalizadas ou aplicando políticas recomendadas pelo fabricante, quando suportado;

14.115.7. A solução deve ser capaz de implantar scripts (por exemplo, PowerShell, Bash e outros) para atender a requisitos de segurança específicos que não estejam disponíveis como funções nativas da própria solução;

14.115.8. A solução deve ser capaz de configurar e implantar políticas de segurança e configuração de endpoints, incluindo: aparência e configurações da área de trabalho do Windows, restrições de navegador, configurações de rede, restrições de acesso ao Painel de

Controle e Gerenciador de Tarefas e controle do menu Iniciar, quando suportado via políticas ou scripts;

14.115.9. A solução deverá disponibilizar funcionalidades nativas de monitoramento contínuo e gerenciamento remoto das cargas de trabalho protegidas, permitindo acompanhamento proativo do estado operacional dos sistemas, sem dependência de ferramentas de terceiros;

14.115.10. O monitoramento deverá abranger, no mínimo:

14.115.10.1. disponibilidade de sistemas e serviços;

14.115.10.2. uso de recursos (CPU, memória, disco);

14.115.10.3. estado de agentes e componentes da solução;

14.115.10.4. falhas recorrentes ou degradação de desempenho.

14.115.11. Deverá possibilitar a automação de ações corretivas a partir de alertas, tais como reinício de serviços, aplicação de correções, notificações ou abertura de chamados, reduzindo tempo médio de resposta a incidentes;

14.115.12. Sempre que possível, as funcionalidades de monitoramento, backup, segurança e recuperação de desastres deverão estar integradas em um único console de administração, com políticas unificadas e visão consolidada do ambiente.

14.116. Relatórios de Utilização de Software e Licenças:

14.116.1. A solução deve ser capaz de rastrear aplicações instaladas em cada agente, identificando quais são efetivamente executadas, para fins de gestão de uso e otimização de licenças;

14.116.2. A solução deve ser capaz de registrar e gerir contratos de licença com base em títulos de software, incluindo: custo da licença, quantidade de licenças, datas de compra e expiração, quando estes dados forem fornecidos pelos administradores;

14.116.3. A solução deve ser capaz de criar relatórios de conformidade de licenças com base nos detalhes especificados nos contratos registrados, correlacionando uso real e licenças disponíveis;

14.116.4. A solução deve ser capaz de gerar relatórios de medição de uso de software, identificando padrões de consumo e ociosidade;

14.116.5. A solução deve ser capaz de gerar relatórios de conformidade de licença para múltiplas plataformas de sistemas operacionais presentes no ambiente.

14.117. Gestão de Vulnerabilidades e Conformidade:

14.117.1. A solução deve identificar e avaliar riscos decorrentes de vulnerabilidades disseminadas na rede, correlacionando inventário de software/OS com bancos de vulnerabilidades suportados pelo fabricante;

14.117.2. A solução deve apoiar a conformidade com padrões de segurança (como CIS Benchmarks) por meio de políticas, scripts e verificações automatizadas, identificando violações e exibindo informações detalhadas sobre medidas corretivas recomendadas;

14.117.3. A solução deve apoiar a identificação e mitigação de vulnerabilidades de zero-day por meio de scripts pré-construídos, políticas de bloqueio e uso combinado dos recursos de segurança (NGAV, anti-ransomware, controle de processos) da plataforma;

14.117.4. A solução deve detectar configurações inseguras, como certificados SSL expirados, permissões inadequadas em diretórios web e outras falhas em servidores, quando suportadas pelas capacidades de varredura da solução;

14.117.5. A solução deve analisar e permitir a desinstalação de softwares inseguros, não autorizados ou sem suporte do fornecedor, de acordo com políticas definidas pelos administradores;

14.117.6. A solução deve gerar informações sobre sistemas nos quais ferramentas de segurança essenciais (como antivírus/NGAV ou agente de proteção da própria solução) estejam ausentes, inativas ou desatualizadas;

14.117.7. A solução deve monitorar portas em uso e processos associados, permitindo identificar serviços expostos e potenciais riscos.

14.118. Segurança de Navegador e Controle de Aplicações:

14.118.1. A solução deve permitir gerenciar a instalação e o uso de extensões e plugins de navegador por meio de políticas, scripts ou configurações, restringindo itens não autorizados;

14.118.2. A solução deve possibilitar controlar o acesso à internet em endpoints, fornecendo ou negando acesso a sites específicos ou categorias de sites, diretamente ou em integração com recursos de proteção web da plataforma;

14.118.3. A solução deve restringir o download de arquivos de sites não autorizados, contribuindo para uma navegação segura em conjunto com os módulos de segurança de conteúdo da solução;

14.118.4. A solução deve permitir a aplicação de políticas que direcionem automaticamente aplicações web legadas para navegadores compatíveis ou emuladores, quando a organização necessitar desse tipo de controle;

14.118.5. A solução deve permitir associar versões específicas de componentes (como Java) às aplicações web que os exijam, sempre que tecnicamente viável e suportado, reduzindo riscos de incompatibilidade e vulnerabilidades;

14.118.6. A solução deve permitir gerenciar favoritos, definir navegadores padrão, configurar políticas para aprimorar segurança do navegador e personalizar configurações de navegação em endpoints;

14.118.7. A solução deve ser capaz de impor modos específicos de navegação (por exemplo, modo restrito ou lista de sites permitidos), garantindo que o endpoint acesse apenas sites autorizados e aplicações web corporativas;

14.118.8. A solução deve detectar o status de conformidade dos computadores em relação a configurações críticas de segurança de navegador e aplicações, sinalizando desvios;

14.118.9. A solução deve suportar a criação de listas de permissões para aplicações, definindo regras de controle com base em pré-requisitos (como editor confiável, localização, hash, assinatura digital);

14.118.10. A solução deve reduzir riscos de ataques cibernéticos bloqueando aplicações não comerciais, executáveis maliciosos e softwares não autorizados, em alinhamento com o módulo de NGAV/EDR da plataforma;

14.118.11. A solução deve ajudar a prevenir ataques de elevação de privilégio, permitindo atribuir acesso privilegiado apenas para aplicações específicas, com base em políticas de menor privilégio;

14.118.12. A solução deve permitir regular o nível de flexibilidade desejado na aplicação das políticas de controle de aplicações, balanceando segurança e usabilidade;

14.118.13. A solução deve permitir tratar usuários temporários que necessitam de acesso privilegiado, concedendo acesso temporário a aplicações e privilégios que sejam revogados automaticamente após período definido;

14.118.14. A solução deve permitir criar políticas globais que controlem a execução de processos filhos, restringindo cadeias de execução suspeitas;

14.118.15. A solução deve permitir que usuários solicitem acesso a aplicações não gerenciadas, com fluxo de aprovação pelo administrador antes de liberar a execução dessas aplicações;

Solução de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados

14.119. A solução deve permitir análise forense dos eventos nos endpoints (desktops e servidores) e seus componentes, detecção de anomalia(s) e visibilidade de processos, complementando e integrando-se com o EDR existente na instituição na detecção e combate a ransomware;

14.120. A solução deve ser dotada de tecnologia polimórfica de proteção de componentes críticos de software, como estruturas de memória, arquivos de aplicativos ou processos, que serão alterados de forma contínua e imprevisível em tempo de execução, tornando quase impossível para os invasores preverem onde injetar código malicioso ou explorar vulnerabilidades baseadas em memória. A solução não deve depender de assinaturas de ameaças ou ser baseada meramente em comportamento a partir de machine learning e/ou deep learning;

14.121. A solução deve trabalhar de forma complementar ao EDR focando em detecção precoce e bloqueio de processos de ransomware, como estruturas de memória, arquivos de aplicativos ou processos, que são alterados de forma contínua e imprevisível em tempo de execução, tornando impossível às ameaças injetar código malicioso nesses componentes críticos de software;

14.122. A solução deve ter capacidade de recuperação baseado em descriptografia, sem depender de backups ou outras soluções externas;

14.123. A solução não deve depender de pré-configurações baseadas na rede do CONTRATANTE para que identifique associações entre múltiplos elementos para que consiga identificar ameaças;

14.124. A plataforma deverá prover arquitetura escalável, permitindo o crescimento de dispositivos suportados, além dos previstos nesta contratação, por meio da adição de novos sensores e licenciamento;

14.125. Solução deve ser capaz de atuar de forma on-line e off-line, ou seja, não dependendo de conexão constante com a internet;

14.126. A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos;

14.127. A solução deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra-ataques cibernéticos, especialmente EDR, através de API;

14.128. A solução deve permitir a integração, através de APIs, com soluções do tipo SOAR, SIEM;

14.129. Deve ser dotada de única interface gráfica a qual permite o gerenciamento centralizado de todos os componentes da solução;

14.130. A solução deve prover visibilidade de vulnerabilidades dos endpoints, sendo capaz de identificar lacunas de segurança nos endpoints, como softwares de alto risco, configurações incorretas, serviços de rede ocultos, manipulação de contas privilegiadas, etc, relacionando-as com ataques de ransomware;

14.131. A ferramenta deve ser capaz de detectar ofuscação de ameaças e ferramentas de movimentação lateral;

14.132. A ferramenta deve evitar roubo de credenciais via browsers e LSASS Dump;

14.133. A ferramenta deve ser capaz de interromper ataques do tipo UAC Bypass e AMSI Bypass;

14.134. A ferramenta deve impedir a destruição de dados por um ataque do tipo ransomware em suas variantes mais agressivas;

14.135. A ferramenta deve implementar a tecnologia AMTD – Automated Moving Target Defense, capaz de paralisar ataques evasivos em memória, “fileless”, process injection, utilitários de hacking, execução de proxy binário e execução de powershell;

14.136. A solução deve garantir a identificação de ameaças do tipo ransomware capazes de criptografar e/ou destruir arquivos do ambiente através do uso da técnica de arquivos-isca (“decoy files”), gerados pela solução de forma imperceptível para o usuário final, mas que uma vez acessados por qualquer ameaça, a solução consiga identificar de forma inequívoca e tomar as ações apropriadas, freando o ataque antes de comprometimento significativo;

14.137. A solução deve permitir a visualização da trajetória do ataque, identificando o endpoint atacado, a trajetória de execução do ataque com os timestamps dos eventos, relacionando com a técnica correspondente do fremawork Mittre Att&ck;

14.138. A solução deve suportar, oferecendo todas as suas funcionalidades, os seguintes sistemas operacionais:

14.138.1. Windows Server versões 2008 R2, 2012,2016,2019,2022 e posteriores – demonstrar instalação e execução;

14.138.2. Windows 7 SP1, 10, 11 e posteriores – demonstrar instalação e execução;

14.138.3. Red Hat Enterprise Linux versões 8,9 e posteriores;

14.138.4. Ubuntu Linux versões 18.04, 20.04, 22.04, 24.04 e posteriores;

14.138.5. Debian Linux versões 11 e 12;

14.138.6. Oracle Linux versões 7,8 e posteriores;

14.138.7. CentOS Stream 8, 9, 10 e posteriores;

14.138.8. CentOS 8 e posteriores;

14.138.9. Citrix Virtual Apps and;

14.138.10. Desktops 7.0 e acima;

14.138.11. Windows Virtual Desktop for Azure Amazon;

14.138.12. WorkSpaces for Windows 10 Clients.

14.139. A solução deverá suportar, ainda que com funcionalidades restritas, os seguintes sistemas operacionais:

14.139.1. Red Hat Enterprise Linux versões 6 e 7 sem eBPF;

14.139.2. Ubuntu Linux versões 14.04 e 16.04 sem eBPF;

14.139.3. Debian Linux Versões 9 e 10 sem eBPF;

14.139.4. CentOS Linux 7 Sem eBPF.

14.140. A solução deve impedir o roubo/exfiltração de dados sensíveis, detectando no mínimo as seguintes técnicas listadas pelo framework Mittre Att&ck:

14.140.1. Id Técnica: Descrição;

14.140.2. T1567: Exfiltração sobre serviço web. Upload de dados roubados para serviços de cloud T1048: Exfiltração sobre protocolo alternativo. Usa tunelamento DNS ou outros protocolos não padrão para evadir detecção;

14.140.3. T1052: Exfiltração sobre meio físico. Copia dados sensíveis para drives USB ou dispositivos similares;

14.140.4. T1029: Transferência agendada. Automatiza exfiltração de dados fora do expediente para evitar detecção;

14.140.5. T1537: Transferência de dados para conta em cloud. Upload de dados usando credenciais de cloud comprometidas;

14.140.6. T1020: Exfiltração automatizada. Automatiza a coleta e transferência de dados sensíveis;

14.140.7. T1485: Destruição de Dados. Deleta os dados depois da exfiltração para ampliar a pressão do ransomware.

14.141. CARACTERISTICAS GERAIS DA PLATAFORMA:

14.141.1. A solução deve permitir *Threat Hunting* e análise forense, análise comportamental dos eventos nos *endpoints* (desktops e servidores) e seus componentes, detecção de anomalia(s) o e visibilidade de processos, complementando o EDR existente na detecção e combate a *ransomware;*

14.141.2. Não serão aceitos produtos ou serviços *OpenSource;*

14.141.3. Todos os componentes devem ser oficialmente suportados pelo(s) fabricante(s) da solução em acordo com as condições especificadas;

14.141.4. A solução deve ser dotada de tecnologia baseada na técnica AMTD (Automated Moving Target Defense), de mutação de alvos de ataque, afim de impedir ataques oriundos de ameaças conhecidas e desconhecidas, inclusive ataques sutis não identificados pelas tecnologias tradicionais de segurança da informação;

14.141.5. A solução deve ser capaz de impedir ataques de forma autônoma, mesmo de ameaças de comportamento desconhecido, e deverá operar normalmente tanto online quanto offline, mesmo sem conexão à rede externa;

14.141.6. A plataforma deverá prover arquitetura escalável, horizontalmente, permitindo o crescimento de dispositivos suportados, além dos previstos nesta contratação, por meio da adição de novos sensores e licenciamento;

14.141.6.1. A solução deve realizar todas as inspeções, processamento, análise e detecção de anormalidades e gerenciamento localmente, ou seja, poderá ser enviado para fora da rede da CONTRATANTE, apenas a telemetria.

14.141.7. A solução deve ser capaz de tomar ações autônomas de resposta contra ameaças e/ou ataques cibernéticos baseadas na tecnologia AMTD;

14.141.8. A solução deve permitir a gestão de usuários a partir de seu próprio console ou integração com Microsoft Entra ID (antigo Azure Active Directory);

14.141.9. A solução deve ser capaz de integrar-se a soluções de segurança terceiras a fim de permitir ações adicionais de bloqueio contra ataques cibernéticos;

14.141.10. A solução deve permitir a integração, a partir de API's, com soluções do tipo SOAR e SIEM;

14.141.11. Deve ser dotada de única interface gráfica a qual permitirá o gerenciamento centralizado de todos os componentes da solução.

14.142. CARACTERÍSTICAS DE GERENCIAMENTO DA PLATAFORMA:

14.142.1. O gerenciador deve possuir controle de interface gráfica (GUI: Graphical User Interface);

14.142.2. A interface gráfica deve possuir no mínimo:

14.142.2.1. Dashboard com total de eventos;

14.142.2.2. Dashboard com total de eventos bloqueados;

14.142.2.3. Dashboard com total de eventos por range temporal;

14.142.2.4. Página inicial com os eventos mais críticos, contendo informações básicas como nome do dispositivo, ação, caminho lógico, data da ocorrência, data da primeira ocorrência, total de ocorrências iguais, ação tomada;

14.142.2.5. Dashboard com total de dispositivos monitorados;

14.142.2.6. Dashboard com total de dispositivos sem comunicação;

14.142.2.7. Dashboard com total de dispositivos que precisam de atualização;

14.142.2.8. Deve oferecer um dashboard de Vulnerabilidade por Máquina, incluindo indicadores como: quantidade de aplicações vulneráveis, pontuação de risco (score), número de CVEs e nível de criticidade por host;

14.142.2.9. Dashboard de Inventário de Software, com visibilidade das aplicações instaladas nos endpoints monitorados. O painel deve incluir informações sobre o ciclo de vida dos softwares, como o status de suporte (end-of-support), viabilizando uma gestão proativa de riscos e conformidade com as políticas da organização;

14.142.2.10. Área de eventos e seus detalhes como data da ocorrência, ID da ameaça (hash), nome do arquivo, tamanho do arquivo, usuário e ação;

14.142.2.11. Área para cadastro e gerenciamento de usuários, divididos por diferentes roles;

14.142.2.12. Área de configurações com possibilidade de envio dos logs de eventos através de feed;

14.142.2.13. Área de configurações para cadastro de provedor de identidade através de protocolo OpenID ou SAML.

14.142.3. A solução deve exibir o método de ataque correlacionado à matriz MITRE ATT&CK, facilitando a categorização e o entendimento tático da ameaça detectada;

14.142.4. Os logs devem registrar o endereço IP da máquina afetada e o usuário conectado no momento do incidente, permitindo rastreabilidade precisa durante a análise forense;

14.142.5. Os logs devem apresentar a cadeia completa de processos, possibilitando a identificação de execuções manuais, automatizadas ou por scripts maliciosos;

14.142.6. Os logs devem detalhar as DLLs de sistema carregadas e seus respectivos caminhos, fornecendo subsídios técnicos para investigação forense aprofundada;

14.142.7. Deve ser possível configurar o intervalo de comunicação (keep-alive) entre o agente e a console, permitindo ajustes conforme as políticas de rede e desempenho;

14.142.8. A solução deve permitir a personalização da mensagem apresentada ao usuário final durante um bloqueio, garantindo uma comunicação alinhada às diretrizes da organização;

14.142.9. Deve incluir uma página de Aplicações Vulneráveis, exibindo softwares de terceiros instalados nos endpoints com respectivas pontuações EPSS, CVSS, quantidade de CVEs associados e hosts afetados, para priorização eficaz de ações corretivas;

14.142.10. Deve incluir uma página de más configurações (“misconfigurations”), que permita a avaliação das configurações de segurança dos hosts com base na política da organização, diferenciando valores seguros e arriscados, além de oferecer recomendações de correção;

14.142.11. Deve incluir uma página de Softwares de Alto Risco, com visibilidade sobre ferramentas potencialmente maliciosas executadas nos últimos 14 dias, destacando usos indevidos de ferramentas nativas (Living-off-the-Land);

14.142.12. A solução deve permitir a exportação de relatórios gerenciais, incluindo: Relatório Executivo de Risco, Relatório de Vulnerabilidades, Relatório de Incidentes, Relatório de Uso de Licenças e Relatório Executivo Operacional;

14.142.13. A solução deve permitir a exportação de logs de auditoria referentes às ações realizadas na console, incluindo eventos como criação ou alteração de políticas, adição de novos usuários, entre outros. Os logs devem conter, no mínimo, os seguintes campos: data e hora do evento, usuário responsável, categoria, tag e descrição da ação realizada. A exportação deve estar disponível nos formatos CSV e JSON;

14.142.14. A solução deve permitir a criação e o gerenciamento de tokens de autenticação para integração via API, com escopos e permissões personalizáveis;

14.142.15. Deve ser possível configurar um prazo máximo de inatividade para os agentes, de forma que, caso não se comuniquem com a console por mais de x dias, sejam automaticamente removidos;

14.142.16. A solução deve oferecer a opção de anonimização dos logs exportados, com capacidade de mascarar informações sensíveis como nome de usuário, endereço IP e nome do host, garantindo conformidade com políticas de privacidade e com a LGPD;

14.142.17. A solução deve permitir a desinstalação remota do agente diretamente pela console, sem a necessidade de qualquer interação manual no endpoint, facilitando o gerenciamento centralizado dos dispositivos monitorados;

14.142.18. A solução deve ser capaz de identificar e exibir as extensões instaladas nos navegadores (“browsers”) de internet dos endpoints monitorados, permitindo visibilidade sobre possíveis vetores de risco ou uso de complementos não autorizados;

14.142.19. A solução deverá permitir o controle da versão do agente diretamente pelo dashboard, possibilitando a gestão da distribuição de atualizações a partir da própria console. Esse recurso deve permitir bloquear atualizações automáticas e aplicar versões apenas após validação interna, garantindo conformidade com os processos de homologação da organização;

14.142.20. A solução deve disponibilizar, de forma integrada na própria console, um menu centralizado de informações sobre novas atualizações, sem a necessidade de acesso a portais externos. Esse menu deve incluir detalhes sobre novas funcionalidades da console, novas funcionalidades do agente e comunicados de inteligência de ameaças (threat intelligence) fornecidos pelo fabricante, garantindo que a equipe de segurança esteja sempre atualizada com as últimas melhorias e orientações;

14.142.21. A solução deve permitir a utilização de segundo fator de autenticação para logins na interface web;

14.142.22. A solução deve possuir mecanismo de gerenciamento de usurários da interface web permitindo:

14.142.22.1. Criação, modificação ou remoção de usuários;

14.142.22.2. Gerenciamento de permissões dos usuários;

14.142.22.3. Opção de gerar usuário com permissão de leitura apenas.

14.142.23. Deve permitir o envio de e-mails de alertas emitidos pela solução;

14.142.24. Deve permitir o envio de logs para sistemas externos.

Sistema Zero Trust (Confiança Zero), Microsegmentação e Ofuscação

14.143. Caracteristicas Tecnicas:

14.143.1. A solução deverá fornecer um esquema de autenticação e autorização dinâmico que controle o acesso dos usuários aos recursos de TI, com base em critérios dinâmicos e granulares, dentro e fora do perímetro da rede;

14.143.2. Fornecer um esquema baseado no modelo Zero-Trust, onde primeiro faz-se a autenticação e depois a conexão, garantindo o acesso somente aos usuários permitidos para recursos específicos, com autenticação, autorização e validação contextual prévias e revalidação contínua durante toda a sessão;

14.143.3. Controlar o acesso baseado na identidade do usuário e não no IP, permitindo validar exatamente quem realiza os acessos, com validação de origem, destino, tempo e regras predefinidas e dinâmicas;

14.143.4. Controlar o acesso centrado na identidade do usuário (Identity-Based Access Control), eliminando dependência de endereçamento IP, permitindo validação e rastreabilidade completas com base em identidade, dispositivo, origem, destino, horário, contexto operacional e políticas dinâmicas;

14.143.5. Aplicar microsegmentação dinâmica e granular, baseada no conceito de “segmento de um”, garantindo que cada usuário tenha acesso exclusivamente aos recursos explicitamente autorizados;

14.143.6. Realizar validação contínua do contexto de acesso (Continuous Trust Evaluation), considerando postura do dispositivo, localização geográfica, comportamento do usuário, nível de risco e condições corporativas, permitindo ajuste dinâmico, restrição ou revogação do acesso em tempo real;

14.143.7. Implementar o conceito de perímetro individualizado por usuário (Segment of One), em que cada identidade possui um perímetro lógico exclusivo, independente da topologia de rede, com isolamento completo entre sessões e usuários;

14.143.8. Garantir que todos os recursos não autorizados permaneçam invisíveis na rede (dark infrastructure), impedindo descoberta, enumeração ou exploração por usuários não autenticados ou agentes maliciosos;

14.143.9. Proporcionar integração com mecanismos de autenticação forte multifatorial (MFA adaptativo), permitindo fatores adicionais com base em risco, criticidade do recurso e contexto de acesso;

14.143.10. Proporcionar integração de modelos de autenticação forte multifatorial para os diferentes níveis de segurança nos acessos corporativos;

14.143.11. Uma vez autenticado o usuário, múltiplas conexões criptografadas são geradas, de cada usuário, para seus recursos autorizados nas diferentes zonas protegidas por meio de Gateways;

14.143.12. Estabelecer múltiplas conexões seguras e independentes, por túneis criptografados dinâmicos e efêmeros, entre usuário e recursos autorizados, utilizando gateways seguros para segmentação e controle de tráfego;

14.143.13. Possibilitar gerenciamento e manutenção simples de regras de segurança para o acesso aos recursos por meio de tags e agrupamentos lógicos;

14.143.14. Eliminar a possibilidade de movimento lateral (ransomware) nos processos de comunicação entre servidores e estações de trabalho;

14.143.15. Permitir gerenciamento simplificado e escalável das políticas de acesso por meio de tags, atributos, agrupamentos lógicos e automação (Policy-as-Code), facilitando administração, padronização e governança;

14.143.16. Eliminar a possibilidade de movimento lateral (lateral movement) entre ativos da rede, prevenindo propagação de ameaças, especialmente ataques do tipo ransomware, por meio de isolamento de sessões e restrição estrita de comunicação;

14.143.17. Proporcionar conexões a recursos de TI com políticas altamente granulares, limitando a comunicação especificamente aos serviços autorizados, portas e protocolos;

14.143.18. Permitir a criação de regras e condições de acesso baseados em usuários e perfis, com condicionamento e supervisão dinâmicos;

14.143.19. Monitorar e fornecer visibilidade de todas as conexões, contínuas e históricas, para gerenciamento e auditoria;

14.143.20. Assegurar que todas as comunicações entre usuários e recursos sejam limitadas exclusivamente a serviços, portas e protocolos explicitamente autorizados, com políticas altamente granulares e controle rigoroso de tráfego;

14.143.21. Permitir a criação e aplicação de regras de acesso com base em perfis, atributos e contexto dos usuários, com condicionamento dinâmico, automação de decisões e supervisão contínua, incluindo integração com mecanismos de avaliação de risco;

14.143.22. Prover monitoramento contínuo e visibilidade completa de todas as conexões, com registros históricos e em tempo real, capacidade de auditoria detalhada, rastreabilidade e suporte à investigação de incidentes;

14.143.23. Apoiar conformidade com regulamentos relativos à autenticação e validação de usuários, criptografia, segregação de redes/usuários e microsegmentação, entre outros;

14.143.24. Proporcionar redução no tempo de preparação de auditorias ao estabelecer conexões pontuais 1:1 entre recursos e por portas específicas;

14.143.25. Apoiar o processo de integração da solução por meio de procedimentos simples e de fácil integração e configuração com o ambiente de TI, redes de missão crítica, fornecedores e terceiros interconectados e serviços de Cloud;

14.143.26. Apoiar conformidade com normas e regulamentações aplicáveis, por meio de integração com o Sistema de Maturidade, incluindo ISO/IEC 27001, CIS Controls v8, NIST Cybersecurity Framework e LGPD;

14.143.27. Gerenciar centralmente o processo de regulação e condicionamento de acesso aos recursos corporativos com base em cada usuário e seu contexto em tempo real;

14.143.28. Ter modelo agnóstico à localização de recursos, seja em nuvem pública, nuvem privada, datacenter, instalações de clientes etc., mantendo o princípio de segurança das comunicações em qualquer ambiente;

14.143.29. Facilitar a integração e complementação com outras ferramentas no ambiente administrativo de TI, simplificando operação e identificação rápida de problemas;

14.144. Arquitetura Operacional da Solução:

14.144.1. Ter um controlador em ambiente computacional virtual (on-premises ou nuvem) que define recursos de rede, condições de acesso e políticas do usuário;

14.144.2. Utilização de Gateway de acesso virtual (on-premises ou nuvem), permitindo conexões dos clientes com recursos protegidos por comunicação criptografada;

14.144.3. SDP para conexões de Cliente: software que permite aos usuários interagir com os recursos de rede;

14.144.4. Log Server virtual (ex.: Kibana) (on-premises ou nuvem): ambiente apartado para registro das informações das conexões ao sistema e aplicativos de controle;

14.144.5. Utilização de Gateway de acesso virtual (on-premises ou nuvem), responsável por:

14.144.5.1. Estabelecer túneis criptografados (ex.: TLS 1.2/1.3 com PFS) entre clientes e recursos autorizados;

14.144.5.2. Encaminhar tráfego somente para aplicações e serviços permitidos, sem exposição de rede (network-less access);

14.144.5.3. Ocultar recursos não autorizados (modelo “dark infrastructure”), prevenindo varredura e enumeração;

14.144.5.4. Aplicar microsegmentação por sessão (segment of one) e controle por aplicação/porta/protocolo;

14.144.5.5. Suportar alta disponibilidade (HA), escalabilidade horizontal e distribuição geográfica;

14.144.5.6. Operar com balanceamento de carga e resiliência a falhas;

14.144.5.7. Registrar telemetria de sessão para auditoria e integração com plataformas de segurança.

14.144.6. SDP para conexão de Cliente, provendo agente cliente (SDP Client) para endpoints, responsável por:

14.144.6.1. Realizar autenticação forte (incluindo MFA), PAM e estabelecer conexões seguras sob demanda;

14.144.6.2. Receber e aplicar políticas dinâmicas definidas pelo controlador;

14.144.6.3. Criar túneis criptografados efêmeros para acesso aos recursos autorizados;

14.144.6.4. Executar verificações de postura do dispositivo (antivírus, patch level, firewall, compliance);

14.144.6.5. Suportar múltiplos sistemas operacionais (Windows, macOS, Linux e dispositivos móveis);

14.144.6.6. Permitir revalidação contínua da sessão (Continuous Trust Evaluation), com ajuste ou revogação de acesso em tempo real;

14.144.6.7. Integrar com certificados digitais, stores corporativas e soluções de MDM/EMM;

14.144.6.8. Operar com mínimo impacto de performance e experiência transparente ao usuário.

14.144.7. Servidor de Logs e Observabilidade (Log Server / Analytics), em ambiente dedicado (on-premises ou nuvem), incluindo:

14.144.7.1. Registro detalhado de autenticações, autorizações, sessões e atividades de usuários;

14.144.7.2. Armazenamento de logs em formato estruturado, com retenção configurável e integridade assegurada;

14.144.7.3. Visualização por dashboards (ex.: Kibana ou equivalente);

14.144.7.4. Integração com SIEM, SOAR, PAM e antiransomware;

14.144.7.5. Enriquecimento de eventos com contexto e score de risco (integração com Risk Sentinel);

14.144.7.6. Suporte a alertas em tempo real, correlação de eventos e trilhas de auditoria;

14.144.7.7. Exportação via APIs/formatos padrão (Syslog, JSON) para conformidade e investigações.

14.145. Funcionalidades de Segurança:

14.145.1. Possuir pacote único de autenticação (Single-Packet Authorization – SPA) pelo qual o agente do usuário solicita acesso ao controlador, que autentica o dispositivo, avalia credenciais e aplica políticas de acesso com base na pessoa, ambiente e infraestrutura; SPA e agente carregam privilégios usados pelo Gateway para descobrir aplicações compatíveis com o contexto;

14.145.2. Substituir as tradicionais VPNs por sistema robusto para ofuscação e controle, conforme requisitos deste documento;

14.145.3. O controlador deve verificar o contexto do usuário e enviar ao cliente seus privilégios, devolvendo ficha criptográfica assinada com autorizações dinâmicas para recursos permitidos;

14.145.4. Criar dinamicamente um segmento único para cada sessão (microsegmentação), por meio de túneis de rede seguros e criptografados via Gateway até o servidor, com todos os túneis e conexões registrados no Log Server;

14.145.5. Manter ambiente com microsegmento para cada privilégio, permitindo ao usuário alcançar o recurso de TI autorizado de forma segura e criptografada, por meio do respectivo Gateway;

14.145.6. Assegurar que o Gateway mantenha recursos invisíveis para usuários não autorizados ou atacantes, impedindo sua visualização;

14.145.7. Garantir que os Gateways permitam proteção granular de localizações locais ou remotas, com escalabilidade e cobertura da diversidade de componentes de TI, administração centralizada e visibilidade das conexões;

14.145.8. Permitir que Gateways e controladores tenham implementações múltiplas, para alta disponibilidade (HA) ou escalabilidade de desempenho;

14.145.9. Proporcionar escalabilidade de datacenter, permitindo implementação de vários gateways e clusters de serviços;

14.145.10. O controlador deve ter capacidade de balancear conexões entre si, distribuindo carga e possibilitando grande capacidade de conexões simultâneas.

14.146. Sistemas Hipervisores (Virtualizadores), Cloud e Agentes:

14.146.1. Hipervisores (Virtualizadores);

14.146.2. VMware ESXi 6.5 ou superior;

14.146.3. vSphere HÁ;

14.146.4. vMotion;

14.146.5. NSX (opcional);

14.146.6. Recomendado: versões 7.x e 8.x;

14.146.7. KVM (Kernel-based Virtual Machine);

14.146.8. Distribuições suportadas:

14.146.8.1. RHEL / Rocky Linux / AlmaLinux 8.x ou superior;

14.146.8.2. Ubuntu Server 20.04 LTS ou superior.

14.147. Suporte a:

14.147.1. Hyper-V Cluster;

14.147.2. SDN (Software Defined Networking);

14.147.3. Citrix Hypervisor:

14.147.3.1. Citrix Hypervisor (XenServer) 8.x ou superior;

14.147.3.2. Compatível com ambientes VDI e virtualização de aplicações.

14.147.4. Nutanix AHV:

14.147.4.1. Nutanix AOS 5.x ou superior;

14.147.4.2. Recomendado: 6.x (LTS);

14.147.4.3. Integração com Prism Central.

14.147.5. Amazon Web Services (AWS):

14.147.5.1. EC2 (todas as gerações atuais suportadas);

14.147.5.2. VPC, Subnets, Security Groups;

14.147.5.3. Suporte a:

14.147.5.3.1. ALB / NLB;

14.147.5.3.2. Auto Scaling;

14.147.5.3.3. AMIs compatíveis com:

14.147.5.3.3.1. Linux (RHEL, Ubuntu).

14.147.6. Microsoft Azure:

14.147.6.1. Máquinas Virtuais Azure:

14.147.6.1.1. Windows Server 2016, 2019, 2022;

14.147.6.1.2. Linux (Ubuntu 20.04+, RHEL 8+);

14.147.6.1.3. Integração com:

14.147.6.1.3.1. Azure AD (Entra ID);

14.147.6.1.3.2. Azure Virtual Network.

14.147.7. Google Cloud Platform (GCP):

14.147.7.1. Compute Engine:

14.147.7.1.1. Ubuntu 20.04+;

14.147.7.1.2. RHEL 8+.

14.147.7.2. Integração com:

14.147.7.2.1. IAM;

14.147.7.2.2. VPC;

14.147.7.2.3. Agentes (Endpoints Corporativos);

14.147.7.2.4. Windows SO;

14.147.7.2.5. Windows 10 (versão 21H2 ou superior);

14.147.7.2.6. Windows 11 (todas as versões suportadas);

14.147.7.2.7. Windows Server: 2016, 2019, 2022;

14.147.7.2.8. Suporte a:

14.147.7.3. Active Directory;

14.147.7.4. GPO;

14.147.7.5. Certificados digitais;

14.147.7.6. macOS;

14.147.7.7. macOS 11 (Big Sur) ou superior;

14.147.7.8. Compatível com Apple Silicon (M1, M2, M3);

14.147.7.9. Linux.

14.147.8. Distribuições suportadas:

14.147.8.1. Ubuntu 20.04 LTS ou superior;

14.147.8.2. RHEL / Rocky / AlmaLinux 8.x ou superior;

14.147.8.3. CentOS Stream 8 ou superior.

14.147.9. Agentes (Lojas Oficiais / Dispositivos Móveis):

14.147.9.1. Android:

14.147.9.1.1. Android 10 ou superior;

14.147.9.1.2. Distribuição via Google Play Store;

14.147.9.1.3. Suporte a MDM / EMM.

14.147.9.2. macOS (App Store):

14.147.9.2.1. Disponível via Apple App Store;

14.147.9.2.2. Compatível com macOS 11 ou superior.

Serviço de prestação continuada de serviços de Network Operations Center — NOC, destinados ao monitoramento, operação e suporte da infraestrutura tecnológica

14.148. A solução proposta deverá obrigatoriamente atender, no mínimo, a todos os itens e subitens conforme descrição abaixo:

14.148.1. Redes locais e de longa distância;

14.148.2. Links de comunicação;

14.148.3. Roteadores, switches, controladores e equipamentos de conectividade;

14.148.4. Firewalls, exclusivamente quanto à disponibilidade, capacidade e funcionamento operacional;

14.148.5. Servidores físicos e virtuais;

14.148.6. Ambientes de virtualização;

14.148.7. Serviços de nuvem;

14.148.8. Sistemas de armazenamento;

14.148.9. Bancos de dados, quando incluídos no catálogo de serviços;

14.148.10. Aplicações e serviços críticos;

14.148.11. DNS, DHCP, VPN, diretórios e demais serviços de infraestrutura;

14.148.12. Interfaces de integração e serviços publicados na rede;

14.148.13. O serviço deverá contemplar monitoramento, detecção, registro, classificação, diagnóstico inicial, escalonamento, acompanhamento da recuperação e geração de indicadores operacionais;

14.148.14. Bens e serviços que compõem a solução:

14.148.14.1. Para atender às necessidades da CONTRATANTE, a contratada deverá disponibilizar:

14.148.14.1.1. Infraestrutura completa de monitoramento centralizado, incluindo segurança, a qual deve proporcionar visibilidade, controle e gerenciamento de todos os ativos e sistemas desta CONTRATANTE, com seus respectivos desempenhos. Tal infraestrutura deve ser capaz de detectar antecipadamente potenciais gargalos, seja nas comunicações entre todas as unidades do órgão e entre estas e a Internet, seja nos ativos e sistemas de TI.

14.149. O NOC deverá concentrar-se na disponibilidade, desempenho, capacidade e continuidade operacional dos serviços de tecnologia;

14.150. Atividades incluídas:

14.150.1. Monitoramento contínuo;

14.150.2. Gestão de eventos operacionais;

14.150.3. Abertura e atualização de chamados;

14.150.4. Diagnóstico inicial;

14.150.5. Escalonamento para equipes responsáveis;

14.150.6. Execução de procedimentos operacionais autorizados;

14.150.7. Acompanhamento de incidentes;

14.150.8. Validação de recuperação;

14.150.9. Monitoramento de capacidade;

14.150.10. Controle de janelas de manutenção;

14.150.11. Relatórios e indicadores;

14.150.12. Atualização de inventário e documentação;

14.150.13. Apoio à gestão de mudanças.

14.151. Modelo de operação:

14.151.1. Regime de atendimento;

14.151.2. A cobertura deverá ser definida por criticidade;

14.151.3. Quadro de cobertura:

14.151.3.1. Categoria: Crítica. - Serviços essenciais ao funcionamento do órgão. Cobertura recomendada: 24 horas por dia, 7 dias por semana, 365 dias por ano;

14.151.3.2. Categoria: Alta. - Serviços relevantes, com impacto em unidades ou grupos de usuários. Cobertura recomendada: Atendimento estendido e escalonamento fora do horário comercial;

14.151.3.3. Categoria: Média. Serviços departamentais ou não essenciais. Cobertura recomendada: Horário comercial ou conforme catálogo;

14.151.3.4. Categoria: Baixa - Serviços auxiliares e itens sem impacto imediato. Cobertura recomendada: Atendimento em horário administrativo.

14.151.4. A CONTRATANTE deverá aprovar uma matriz de criticidade, relacionando cada ativo ou serviço ao horário de cobertura, prazo de atendimento e grupo responsável.

14.152. Funções da equipe:

14.152.1. A contratada deverá dimensionar equipe suficiente para cumprir os níveis de serviço, contemplando, no mínimo:

14.152.1.1. Operadores de NOC;

14.152.1.2. Líder ou supervisor de turno;

14.152.1.3. Especialistas de segundo nível;

14.152.1.4. Especialistas de terceiro nível, quando necessários;

14.152.1.5. Gestor técnico do serviço;

14.152.1.6. Ponto focal para relacionamento com a CONTRATANTE.

14.152.2. Equipe de transição e documentação:

14.152.2.1. A especificação deve exigir cobertura e capacidade operacional, e não apenas uma quantidade fixa de pessoas;

14.152.2.2. O dimensionamento deve considerar:

14.152.2.2.1. Número de ativos;

14.152.2.2.2. Volume de eventos;

14.152.2.2.3. Quantidade de serviços críticos;

14.152.2.2.4. Horário de cobertura;

14.152.2.2.5. Quantidade de unidades administrativas;

14.152.2.2.6. Necessidade de escalonamento;

14.152.2.2.7. Volume histórico de incidentes;

14.152.2.2.8. Tecnologias utilizadas.

14.152.3. Requisitos funcionais:

14.152.3.1. NOC-F-001 — Inventário de ativos;

14.152.3.2. A solução deverá manter inventário atualizado dos elementos monitorados, contendo, no mínimo:

14.152.3.2.1. Identificação única;

14.152.3.2.2. Nome do ativo;

14.152.3.2.3. Tipo de equipamento ou serviço;

14.152.3.2.4. Fabricante e modelo, quando aplicável;

14.152.3.2.5. Número de série, quando aplicável;

14.152.3.2.6. Endereço IP;

14.152.3.2.7. Endereço IPv6, quando aplicável;

14.152.3.2.8. Localização física ou lógica;

14.152.3.2.9. Unidade administrativa;

14.152.3.2.10. Responsável técnico;

14.152.3.2.11. Serviço associado;

14.152.3.2.12. Grau de criticidade;

14.152.3.2.13. Grupo de atendimento;

14.152.3.2.14. Janela de manutenção;

14.152.3.2.15. Perfil de monitoramento;

14.152.3.2.16. Dependências conhecidas;

14.152.3.2.17. Data de inclusão ou alteração.

14.152.4. NOC-F-002 — Descoberta e atualização deverá permitir:

14.152.4.1. Descoberta automática ou assistida de ativos;

14.152.4.2. Identificação de novos dispositivos;

14.152.4.3. Detecção de alterações de endereço ou configuração;

14.152.4.4. Comparação entre inventário previsto e inventário identificado;

14.152.4.5. Atualização manual e automática;

14.152.4.6. Registro do responsável pela alteração;

14.152.4.7. Integração com base de configuração ou inventário institucional.

14.152.5. NOC-F-003 — Representação de topologia deverá apresentar a topologia física e lógica, incluindo:

14.152.5.1. Relação entre dispositivos;

14.152.5.2. Interfaces;

14.152.5.3. Links;

14.152.5.4. Dependências;

14.152.5.5. Caminhos de comunicação;

14.152.5.6. Sites e unidades;

14.152.5.7. Serviços vinculados aos ativos;

14.152.5.8. Impacto estimado de uma falha.

14.152.6. NOC-F-004 — Monitoramento de disponibilidade deverá monitorar, conforme aplicável:

14.152.6.1. Disponibilidade de equipamentos;

14.152.6.2. Estado de interfaces;

14.152.6.3. Links de comunicação;

14.152.6.4. Serviços TCP e UDP;

14.152.6.5. DNS;

14.152.6.6. DHCP;

14.152.6.7. HTTP e HTTPS;

14.152.6.8. VPN;

14.152.6.9. Servidores;

14.152.6.10. Máquinas virtuais;

14.152.6.11. Armazenamento;

14.152.6.12. Bancos de dados;

14.152.6.13. Aplicações;

14.152.6.14. Serviços de nuvem;

14.152.6.15. APIs e integrações;

14.152.6.16. Deverá ser possível distinguir:

14.152.6.16.1. Equipamento indisponível;

14.152.6.16.2. Interface inativa;

14.152.6.16.3. Perda de conectividade;

14.152.6.16.4. Falha de rota;

14.152.6.16.5. Serviço indisponível;

14.152.6.16.6. Falha de dependência;

14.152.6.16.7. Interrupção programada.

14.152.7. NOC-F-005 — Monitoramento de desempenho deverá coletar e apresentar, quando aplicável:

14.152.7.1. Latência;

14.152.7.2. Perda de pacotes;

14.152.7.3. Variação de atraso;

14.152.7.4. Utilização de banda;

14.152.7.5. Erros e descartes em interfaces;

14.152.7.6. CPU;

14.152.7.7. Memória;

14.152.7.8. Armazenamento;

14.152.7.9. Temperatura;

14.152.7.10. Estado de fontes e ventiladores;

14.152.7.11. Utilização de sessões;

14.152.7.12. Quantidade de conexões;

14.152.7.13. Tempo de resposta de aplicações;

14.152.7.14. Taxa de erro;

14.152.7.15. Tempo de resposta de APIs;

14.152.7.16. Desempenho de máquinas virtuais;

14.152.7.17. Desempenho de dispositivos de armazenamento.

14.152.8. NOC-F-006 — Monitoramento de capacidade deverá permitir:

14.152.8.1. Definição de limites de utilização;

14.152.8.2. Identificação de saturação;

14.152.8.3. Análise histórica;

14.152.8.4. Projeção de crescimento;

14.152.8.5. Identificação de tendência de esgotamento;

14.152.8.6. Relatórios de capacidade;

14.152.8.7. Recomendações de expansão;

14.152.8.8. Comparação entre capacidade contratada e consumo real;

14.152.8.9. Deverão ser acompanhados, no mínimo:

14.152.8.9.1. Capacidade de links;

14.152.8.9.2. Processamento;

14.152.8.9.3. Memória;

14.152.8.9.4. Armazenamento;

14.152.8.9.5. Quantidade de sessões;

14.152.8.9.6. Endereços disponíveis;

14.152.8.9.7. Recursos de virtualização;

14.152.8.9.8. Licenças ou cotas técnicas, quando aplicável.

14.152.9. NOC-F-007 — Coleta de eventos deverá receber eventos provenientes de:

14.152.9.1. Equipamentos de rede;

14.152.9.2. Servidores;

14.152.9.3. Sistemas operacionais;

14.152.9.4. Plataformas de virtualização;

14.152.9.5. Serviços de nuvem;

14.152.9.6. Aplicações;

14.152.9.7. Bancos de dados;

14.152.9.8. Ferramentas de inventário;

14.152.9.9. Sistemas de chamados;

14.152.9.10. APIs;

14.152.9.11. Plataformas de gerenciamento;

14.152.9.12. Cada evento deverá possuir, sempre que possível:

14.152.9.12.1. Data e hora;

14.152.9.12.2. Origem;

14.152.9.12.3. Categoria;

14.152.9.12.4. Severidade;

14.152.9.12.5. Estado;

14.152.9.12.6. Descrição;

14.152.9.12.7. Ativo relacionado;

14.152.9.12.8. Serviço afetado;

14.152.9.12.9. Regra que gerou o evento;

14.152.9.12.10. Chamado associado;

14.152.9.12.11. Ação executada;

14.152.9.12.12. Responsável pelo tratamento.

14.152.10. NOC-F-008 — Protocolos e métodos de coleta deverão suportar, conforme a infraestrutura do órgão:

14.152.10.1. ICMP para disponibilidade e latência;

14.152.10.2. SNMPv3 para coleta de métricas;

14.152.10.3. SNMPv2c somente quando houver equipamento legado e justificativa técnica;

14.152.10.4. Syslog;

14.152.10.5. NetFlow ou IPFIX;

14.152.10.6. HTTP e HTTPS;

14.152.10.7. DNS;

14.152.10.8. TCP e UDP;

14.152.10.9. APIs REST;

14.152.10.10. Webhooks;

14.152.10.11. Agentes de monitoramento;

14.152.10.12. SSH ou mecanismos equivalentes para diagnóstico autorizado;

14.152.10.13. Telemetria nativa dos fabricantes;

14.152.10.14. Protocolos específicos de virtualização e nuvem;

14.152.10.15. A utilização de credenciais de escrita deverá ser excepcional. O padrão deverá ser:

14.152.10.15.1. Acesso de leitura;

14.152.10.15.2. Contas individuais;

14.152.10.15.3. Autenticação forte;

14.152.10.15.4. Registro de sessão;

14.152.10.15.5. Aprovação prévia para ações modificadoras;

14.152.10.15.6. Utilização de mecanismo intermediário de acesso quando necessário.

14.152.11. NOC-F-009 — Correlação e deduplicação deverá:

14.152.11.1. Agrupar eventos relacionados;

14.152.11.2. Identificar dependências;

14.152.11.3. Evitar abertura de múltiplos chamados para a mesma causa;

14.152.11.4. Suprimir eventos derivados de uma falha principal;

14.152.11.5. Diferenciar falha real de evento transitório;

14.152.11.6. Permitir regras configuráveis;

14.152.11.7. Associar eventos a serviços afetados;

14.152.11.8. Reabrir o incidente quando a falha retornar.

14.152.12. NOC-F-010 — Classificação de criticidade deverão ser classificados, no mínimo, em:

14.152.12.1. Crítico;

14.152.12.2. Alto;

14.152.12.3. Médio;

14.152.12.4. Baixo;

14.152.12.5. Informativo;

14.152.12.6. A classificação deverá considerar:

14.152.12.6.1. Impacto;

14.152.12.6.2. Urgência;

14.152.12.6.3. Quantidade de usuários afetados;

14.152.12.6.4. Quantidade de unidades afetadas;

14.152.12.6.5. Relevância do serviço;

14.152.12.6.6. Duração;

14.152.12.6.7. Existência de contingência;

14.152.12.6.8. Dependência de outros serviços.

14.152.13. NOC-F-011 — Limiares e alertas deverão permitir configurar:

14.152.13.1. Limiares fixos;

14.152.13.2. Limiares por horário;

14.152.13.3. Limiares por ativo;

14.152.13.4. Limiares por serviço;

14.152.13.5. Limiares dinâmicos;

14.152.13.6. Períodos de tolerância;

14.152.13.7. Histerese;

14.152.13.8. Alertas por persistência;

14.152.13.9. Alertas por tendência;

14.152.13.10. Alertas de ausência de dados;

14.152.13.11. Alertas de recuperação;

14.152.13.12. Os limiares deverão ser revisados periodicamente para reduzir falsos positivos e alertas sem ação operacional.

14.152.14. NOC-F-012 — Janelas de manutenção deverá permitir o cadastro de:

14.152.14.1. Data e horário de início;

14.152.14.2. Data e horário de encerramento;

14.152.14.3. Ativos envolvidos;

14.152.14.4. Serviços afetados;

14.152.14.5. Responsável;

14.152.14.6. Motivo;

14.152.14.7. Número da mudança ou ordem de serviço;

14.152.14.8. Procedimento de validação;

14.152.14.9. Procedimento de reversão;

14.152.14.10. Durante a manutenção, os alertas deverão ser tratados conforme a regra aprovada, sem perda do histórico de eventos.

14.152.15. NOC-F-013 — Monitoramento sintético, quando aplicável, deverão ser realizados testes periódicos de:

14.152.15.1. Resolução de nomes;

14.152.15.2. Conectividade;

14.152.15.3. Disponibilidade de portas;

14.152.15.4. Acesso HTTP e HTTPS;

14.152.15.5. Tempo de resposta;

14.152.15.6. Autenticação em aplicações autorizadas;

14.152.15.7. Disponibilidade de APIs;

14.152.15.8. Transações críticas não invasivas.

14.152.16. NOC-F-014 — Gestão de incidentes ao identificar evento relevante, o NOC deverá:

14.152.16.1. Validar o evento;

14.152.16.2. Identificar o ativo ou serviço afetado;

14.152.16.3. Classificar impacto e urgência;

14.152.16.4. Abrir ou vincular chamado;

14.152.16.5. Executar o diagnóstico inicial;

14.152.16.6. Acionar o grupo responsável;

14.152.16.7. Acompanhar a evolução;

14.152.16.8. Atualizar as partes interessadas;

14.152.16.9. Validar a normalização;

14.152.16.10. Registrar a causa aparente e as ações realizadas;

14.152.16.11. Encerrar o chamado conforme critérios definidos.

14.152.17. NOC-F-015 — Integração com sistema de chamados deverá integrar-se ao sistema de gestão de serviços utilizado pelo órgão, quando for o caso, permitindo:

14.152.17.1. Abertura automática de chamados;

14.152.17.2. Atualização de chamados;

14.152.17.3. Inclusão de evidências;

14.152.17.4. Associação entre evento e chamado;

14.152.17.5. Alteração de prioridade;

14.152.17.6. Escalonamento;

14.152.17.7. Registro de comentários;

14.152.17.8. Encerramento após validação;

14.152.17.9. Sincronização do estado do evento;

14.152.17.10. Consulta do histórico.

14.152.18. NOC-F-016 — Escalonamento deverá existir matriz de escalonamento contendo:

14.152.18.1. Equipe de primeiro atendimento;

14.152.18.2. Equipe técnica responsável;

14.152.18.3. Gestor do serviço;

14.152.18.4. Responsável da unidade;

14.152.18.5. Fornecedor de telecomunicações;

14.152.18.6. Fabricante ou suporte especializado;

14.152.18.7. Autoridade a ser comunicada em incidentes críticos;

14.152.18.8. Prazo para escalonamento;

14.152.18.9. Canal de comunicação;

14.152.18.10. Procedimento fora do horário comercial.

14.152.19. NOC-F-017 — Procedimentos operacionais deverão manter procedimentos documentados para os eventos recorrentes, incluindo:

14.152.19.1. Sintoma;

14.152.19.2. Causa provável;

14.152.19.3. Evidências a coletar;

14.152.19.4. Comandos ou verificações autorizadas;

14.152.19.5. Riscos;

14.152.19.6. Critério de escalonamento;

14.152.19.7. Procedimento de recuperação;

14.152.19.8. Critério de encerramento;

14.152.19.9. Necessidade de comunicação;

14.152.19.10. Relação com mudanças ou problemas conhecidos.

14.152.20. NOC-F-018 — Automação controlada a execução automatizada de comandos ou procedimentos deverá:

14.152.20.1. Ser previamente autorizada;

14.152.20.2. Possuir escopo definido;

14.152.20.3. Utilizar credenciais apropriadas;

14.152.20.4. Registrar data, hora e operador;

14.152.20.5. Registrar o comando ou procedimento;

14.152.20.6. Possuir mecanismo de interrupção;

14.152.20.7. Possuir validação posterior;

14.152.20.8. Possuir procedimento de reversão;

14.152.20.9. Ser limitada a ativos autorizados.

14.152.21. NOC-F-019 — Validação de mudanças o NOC deverá executar verificações de:

14.152.21.1. Disponibilidade;

14.152.21.2. Latência;

14.152.21.3. Rotas;

14.152.21.4. Interfaces;

14.152.21.5. Consumo de recursos;

14.152.21.6. Serviços relacionados;

14.152.21.7. Integrações;

14.152.21.8. Alarmes gerados;

14.152.21.9. Capacidade;

14.152.21.10. Funcionamento da contingência, quando aplicável.

14.152.22. NOC-F-020 — Painéis operacionais deverão disponibilizar painéis para:

14.152.22.1. Situação geral da infraestrutura;

14.152.22.2. Serviços críticos;

14.152.22.3. Incidentes abertos;

14.152.22.4. Ativos indisponíveis;

14.152.22.5. Links e interfaces;

14.152.22.6. Capacidade;

14.152.22.7. Eventos por severidade;

14.152.22.8. Incidentes por unidade;

14.152.22.9. Tendências;

14.152.22.10. Cumprimento de níveis de serviço;

14.152.22.11. Situação das ferramentas de monitoramento;

14.152.22.12. Os painéis deverão permitir filtros por:

14.152.22.12.1. Unidade;

14.152.22.12.2. Serviço;

14.152.22.12.3. Tecnologia;

14.152.22.12.4. Fabricante;

14.152.22.12.5. Criticidade;

14.152.22.12.6. Período;

14.152.22.12.7. Grupo responsável;

14.152.22.12.8. Estado do evento.

14.152.23. Requisitos de arquitetura:

14.152.23.1. Arquitetura distribuída para órgãos com múltiplas unidades ou redes geograficamente distribuídas, a solução deverá permitir:

14.152.23.1.1. Coletores ou sondas distribuídas;

14.152.23.1.2. Coleta local em caso de indisponibilidade do enlace;

14.152.23.1.3. Sincronização posterior;

14.152.23.1.4. Administração centralizada;

14.152.23.1.5. Redundância dos componentes críticos;

14.152.23.1.6. Monitoramento dos próprios coletores;

14.152.23.1.7. Operação em ambientes locais, virtualizados e em nuvem.

14.152.24. Alta disponibilidade:

14.152.24.1. A plataforma deverá evitar ponto único de falha nos seguintes componentes:

14.152.24.1.1. Servidor de gerenciamento;

14.152.24.1.2. Banco de dados;

14.152.24.1.3. Armazenamento;

14.152.24.1.4. Coletores;

14.152.24.1.5. Interfaces de integração;

14.152.24.1.6. Sistema de chamados;

14.152.24.1.7. Canais de comunicação.

14.152.25. Mecanismos de autenticação deverá gerar alerta quando o próprio monitoramento estiver degradado ou interrompido:

14.152.25.1. O dimensionamento deverá considerar uma margem de expansão, evitando que a plataforma opere permanentemente próxima da capacidade máxima.

14.152.26. Níveis de serviço cuja matriz abaixo é um modelo de referência:

14.152.26.1. P1 — Crítica. Situação: Indisponibilidade total de serviço essencial ou impacto amplo. Reconhecimento: Até 5 min. Atualização: A cada 30 min. Escalonamento: Imediato;

14.152.26.2. P2 — Alta. Situação: Degradação relevante ou impacto em unidade importante. Reconhecimento: Até 15 min. Atualização: A cada 60 min. Escalonamento: Até 30 min;

14.152.26.3. P3 — Média. Situação: Impacto limitado ou falha sem interrupção crítica. Reconhecimento: Até 60 min. Atualização: Conforme evolução. Escalonamento: Até 4 h;

14.152.26.4. Baixa. Situação: Solicitação, informação ou evento sem impacto operacional. Reconhecimento: Até 4 h úteis. Atualização: Conforme necessidade. Escalonamento: Conforme catálogo.

14.152.27. A CONTRATANTE deverá definir separadamente:

14.152.27.1. Tempo de reconhecimento;

14.152.27.2. Tempo de diagnóstico inicial;

14.152.27.3. Tempo de escalonamento;

14.152.27.4. Tempo de comunicação;

14.152.27.5. Tempo de restauração;

14.152.27.6. Tempo de solução definitiva;

14.152.27.7. Prazo de entrega de relatório;

14.152.27.8. Tratamento de reincidência;

14.152.27.9. Critérios de exclusão de indisponibilidade;

14.152.27.10. Janelas de manutenção autorizadas;

14.152.27.11. Quando a restauração depender de terceiro, fornecedor de telecomunicações ou equipe do órgão, a contratada deverá continuar responsável por:

14.152.27.11.1. Detectar o problema;

14.152.27.11.2. Registrar o incidente;

14.152.27.11.3. Acionar o responsável;

14.152.27.11.4. Acompanhar o atendimento;

14.152.27.11.5. Atualizar os interessados;

14.152.27.11.6. Registrar a linha do tempo;

14.152.27.11.7. Validar a normalização.

14.152.28. Entregáveis obrigatórios, a contratada deverá entregar, no mínimo:

14.152.28.1. Plano de implantação que deverá conter:

14.152.28.1.1. Cronograma;

14.152.28.1.2. Equipe;

14.152.28.1.3. Responsabilidades;

14.152.28.1.4. Dependências;

14.152.28.1.5. Riscos;

14.152.28.1.6. Estratégia de migração;

14.152.28.1.7. Plano de comunicação;

14.152.28.1.8. Critérios de aceite;

14.152.28.1.9. Plano de contingência.

14.152.28.2. Inventário inicial deverá apresentar:

14.152.28.2.1. Ativos identificados;

14.152.28.2.2. Ativos previstos;

14.152.28.2.3. Ativos sem monitoramento;

14.152.28.2.4. Serviços associados;

14.152.28.2.5. Responsáveis;

14.152.28.2.6. Criticidade;

14.152.28.2.7. Cobertura planejada;

14.152.28.2.8. Pendências de acesso ou documentação.

14.152.29. Matriz de monitoramento para cada ativo ou serviço:

14.152.29.1. Item monitorado;

14.152.29.2. Métrica;

14.152.29.3. Fonte;

14.152.29.4. Periodicidade;

14.152.29.5. Limite de alerta;

14.152.29.6. Severidade;

14.152.29.7. Grupo responsável;

14.152.29.8. Procedimento associado;

14.152.29.9. Janela de manutenção;

14.152.29.10. Critério de normalização.

14.152.30. Catálogo de serviços deverá relacionar:

14.152.30.1. Nome do serviço;

14.152.30.2. Descrição;

14.152.30.3. Usuários;

14.152.30.4. Unidade responsável;

14.152.30.5. Ativos dependentes;

14.152.30.6. Criticidade;

14.152.30.7. Horário de atendimento;

14.152.30.8. Meta de disponibilidade;

14.152.30.9. Procedimento de escalonamento;

14.152.30.10. Plano de contingência.

14.152.31. Relatório mensal deverá conter:

14.152.31.1. Disponibilidade por serviço;

14.152.31.2. Incidentes ocorridos;

14.152.31.3. Incidentes críticos;

14.152.31.4. Cumprimento de prazos;

14.152.31.5. Tempo de reconhecimento;

14.152.31.6. Tempo de restauração;

14.152.31.7. Alertas gerados;

14.152.31.8. Falsos positivos;

14.152.31.9. Eventos recorrentes;

14.152.31.10. Capacidade;

14.152.31.11. Tendências;

14.152.31.12. Manutenções realizadas;

14.152.31.13. Pendências;

14.152.31.14. Riscos;

14.152.31.15. Recomendações;

14.152.31.16. Relatório de causa e melhoria;

14.152.31.17. Para incidentes críticos ou recorrentes, deverá ser produzido relatório contendo:

14.152.31.17.1. Linha do tempo;

14.152.31.17.2. Serviço afetado;

14.152.31.17.3. Impacto;

14.152.31.17.4. Causa provável ou confirmada;

14.152.31.17.5. Evidências;

14.152.31.17.6. Ações executadas;

14.152.31.17.7. Tempo de indisponibilidade;

14.152.31.17.8. Falhas de detecção;

14.152.31.17.9. Medidas corretivas;

14.152.31.17.10. Medidas preventivas;

14.152.31.17.11. Responsáveis;

14.152.31.17.12. Prazo de conclusão;

14.152.31.17.13. Validação.

14.152.32. Gestão de mudanças deverá possuir:

14.152.32.1. Identificação;

14.152.32.2. Justificativa;

14.152.32.3. Responsável;

14.152.32.4. Data e horário;

14.152.32.5. Escopo;

14.152.32.6. Impacto previsto;

14.152.32.7. Risco;

14.152.32.8. Plano de execução;

14.152.32.9. Plano de reversão;

14.152.32.10. Plano de validação;

14.152.32.11. Comunicação;

14.152.32.12. Evidências pós-mudança.

14.152.33. O NOC deverá verificar se a mudança:

14.152.33.1. Gerou novos alertas;

14.152.33.2. Causou indisponibilidade;

14.152.33.3. Alterou a topologia;

14.152.33.4. Modificou a capacidade;

14.152.33.5. Afetou dependências;

14.152.33.6. Exige atualização de inventário;

14.152.33.7. Exige atualização de procedimentos.

CARACTERÍSTICAS GERAIS DOS FIREWALLS FÍSICOS

14.153. Todos os firewalls modelos I, II,II e IV deverão atender obrigatoriamente a todos os requisitos técnicos listados neste Termo de Referência;

14.154. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, prevenção de ataques zero-day, filtro de URL, identificação de usuários e controle granular de permissões;

14.155. Para proteção do ambiente contra ataques, o dispositivo de proteção deve possuir módulos de IPS, Antivírus e Anti-Spyware (para bloqueio de arquivos maliciosos), integrados ao próprio appliance de NGFW;

14.156. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;

14.157. Define-se o termo “appliance” como sendo um equipamento dotado de processamento, memória e outros recursos tecnológicos exclusivos para um determinado serviço. Um appliance é projetado para executar uma tarefa específica de forma eficiente e simplificada, com recursos e software otimizados para essa finalidade;

14.158. Não serão aceitas soluções baseadas em PC's (personal computers) de uso geral, assim como, soluções de “appliance” que utilizam hardware e software de fabricantes diferentes;

14.159. Os firewalls devem ser entregues com licencimanto válido para, no mínimo, 12 meses, incluindo garantia e suporte;

14.160. Deve ser capaz de atualizar de forma automática o Firmware, patches e atualizções de segurança;

14.161. A solução deve permitir o uso de armazenamento externo para System Logs, Threat Logs, AppFlow reporting data e Packet Captures, garantindo persistência de dados após reinicializações do firewall;

14.162. O painel deve exibir detalhes sobre o último contato do Firewall com o gerenciador de licenciamento, mostrando o status de atualização de licenças e atualizações de assianturas;

14.163. Deve fornece APIs para que os fornecedores externos de NAC possam transmitir o contexto de segurança aos firewalls e que estea funcionalidade seja compatível com a utilização simultânea de fornecedores externos distintos;

14.164. A solução de segurança não pode aplicar nenhum tipo de exceção de inspeção de tráfego (bypass) oriunda de condições de limitação de capacidade de processamento de forma automática. Toda e qualquer exceção (bypass) de inspeção e tráfego deve ser possível apenas através de ação explícita e específica criada pelo administrador da plataforma através de configurações realizadas pela console gráfica do appliance, ou pela plataforma centralizada de gerenciamento da solução;

14.165. CARACTERÍSTICAS DIVERSAS:

14.165.1. Deve implementar controle do tráfego para os protocolos TCP, UDP, ICMP, e serviços como FTP, DNS, P2P entre outros, baseados nos endereços de origem e destino;

14.165.2. Implementar recurso de NAT (network address translation) tipo one-to-one, one-to-many, many-to-many, many-to-one, porta TCP de conexão (NAPT) e NAT Traversal em VPN IPSec (NAT-T) e NAT dentro do tunel IPSec;

14.165.3. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;

14.165.4. Deve possuir proteção anti-spoofing;

14.165.5. Suportar protocolos de roteamento RIP, RIPng, OSPF, OSPFv3 e BGP;

14.165.6. Suportar Equal Cost Multi-Path (ECMP) no mínimo para roteamento estático e protocolo OSPF;

14.165.7. Suporte a Policy-Based Routing (PBR), com a capacidade de roteamento no mínimo, mas não limitado a: endereço de origem, endereço de destino, serviço e aplicação;

14.165.8. A solução deverá possuir a tecnologia SD-WAN (Software Defined WAN), e que a mesma seja nativa da solução, sem a necessidade de qualquer tipo de licenciamento complementar, para evitar indisponibilidade no ambiente mesmo em caso de expiração do licenciamento vigente;

14.165.9. Capacidade de agregar no mínimo 4 (quatro) circuitos WAN distintos em um único canal lógico onde seja possível criar controles de caminho automático baseado em políticas, com habilidade de selecionar o melhor caminho, no mínimo, através dos seguintes parâmetros simultâneos:

14.165.9.1. Latência;

14.165.9.2. Jitter;

14.165.9.3. Perda de pacotes.

14.165.10. O administrador da solução deverá ter a capacidade de configurar o canal lógico de SD-WAN para encaminhar tráfego simultaneamente por todos os links pertencentes a esse canal logico;

14.165.11. A comutação do SD-WAN deve ocorrer de maneira dinâmica e automática baseada nas políticas previamente aplicadas;

14.165.12. A solução de SD-WAN deve permitir encaminhamento de trafego com base em assinaturas de aplicações conhecidas (DPI), como Office 365, Facebook e Youtube, bem como aplicações associadas como Facebook Messenger e Office 365 Outlook;

14.165.13. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;

14.165.14. Deve suportar modo misto de trabalho Sniffer, L2 e L3 em diferentes interfaces físicas;

14.165.15. Implementar proxy transparente para o protocolo HTTP, de forma a dispensar a configuração dos browsers das máquinas clientes;

14.165.16. Possuir servidor de DHCP (Dynamic Host Configuration Protocol) interno com capacidade de alocação de endereçamento IP para as estações conectadas às interfaces do firewall e via VPN;

14.165.17. Deve suportar DHCP relay;

14.165.18. Possibilitar a aplicação de regras de firewall e IPS por IP e grupo de usuários, permitindo a definição de regras para determinado horário ou período (dia da semana e hora) com matriz de horários que possibilite o bloqueio de serviços em horários específicos, tendo o início e fim das conexões vinculadas a essa matriz de horários;

14.165.19. Deve permitir a utilização de regras de Anti-Vírus, Anti-Spyware, IPS e filtro de conteúdo web por segmentos de rede. Todos os serviços devem ser suportados no mesmo segmento de rede, interface (fisica e virtual) ou zona de segurança;

14.165.20. Possuir capacidade de inspecionar e bloquear em tempo real aplicativos e transferências de arquivos de softwares p2p (peer-to-peer) incluindo, no mínimo, Kazaa, Limewire, Morpheus e Napster e de comunicadores instantâneos (instant messengers) incluindo, no mínimo, ICQ, WhatsApp, Google Talk, Skype e IRC, para usuários da rede, individualmente ou em grupo;

14.165.21. Deve ter suporte a proteção e identificação de hosts possivelmente infectados com “botnets”. A solução ofertada deve permitir ao administrador a possibilidade de apenas registrar e identificar as máquinas possivelmente contaminadas, além de ter a possibilidade de habilitar e analisar todas as conexões que passam por este dispositivo de segurança, bem como ativar tal funcionalidade especificando análise por regra de firewall, permitindo assim maior granularidade da gestão e do recurso;

14.165.22. Possuir assinaturas específicas, ou implementar mecanismo interno no appliance, para mitigação de ataques DoS (denial-of-service) e DDoS devidamente licenciados;

14.165.23. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

14.165.24. Detectar e bloquear a origem de portscans;

14.165.25. Deve permitir o bloqueio de ataques;

14.165.26. Deve permitir o bloqueio de exploits conhecidos;

14.165.27. O gateway Anti-Vírus deve suportar a análise de pelo menos os protocolos HTTP, FTP, IMAP, e SMTP;

14.165.28. Deve ter a capacidade de analisar tráfegos criptografados HTTPS/SSL, que deverá ser decriptografado de forma transparente à aplicação;

14.165.29. Implementar DSCP (Differentiated Services Code Points);

14.165.30. Possuir mecanismo de forma a possibilitar o funcionamento transparente dos protocolos FTP, SIP, RTP, RTSP e H323, mesmo quando acessados por máquinas através de conversão de endereços. Este suporte deve funcionar tanto para acessos de dentro para fora quanto de fora para dentro da rede;

14.165.31. Implementar controle e gerenciamento de banda para a tecnologia VoIP(Voice OverIP) sobre diferentes segmentos de rede com inspeção profunda de segurança sobre este serviço;

14.165.32. Implementar mecanismo de sincronismo de horário através do protocolo NTP;

14.165.33. Possuir suporte ao protocolo SNMP versões 2 e 3;

14.165.34. Possuir suporte a log via syslog;

14.165.35. Possuir suporte aos protocolos de roteamento RIP, OSPF e BGP. As configurações de RIP e OSPF devem ser configuradas através da interface gráfica;

14.165.36. Reconhecer aplicações como, no mínimo, peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos e e-mail;

14.165.37. Controle, inspeção e de-criptografia de SSL/TLS por política para tráfego de entrada (Inbound) ou Saída (Outbound) com suporte a no mínimo, SSLv23, SSLv3, TLS 1.2 e TLS 1.3;

14.165.38. Deve permitir a funcionalidade de ARP bridging;

14.165.39. Deve permitir a configuração de limite na taxa de envio ARP para um mesmo IP, para evitar "ARP Storm";

14.165.40. A solução deve permitir a visualização gráfica das regras de segurança e acesso;

14.165.41. O equipamento deverá prover a funcionalidade de servidor NTP (Network Time Protocol) para sincronização precisa de data e hora dos dispositivos da rede;

14.165.42. Para os modelos de firewall que por ventura sejam entregues com funcionalidade wireless, o equipamento deverá suportar os padrões de segurança WPA2/WPA3 Enterprise e protocolo de autenticação EAP em modo estação, oferecendo maior proteção para as conexões sem fio;

14.165.43. O firewall deverá implementar a funcionalidade de DNS proxy para otimizar e controlar as requisições de resolução de nomes de domínio na rede.

14.166. CARACTERÍSTICAS DE VPN:

14.166.1. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo site-to-site, com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

14.166.2. Suportar algoritmos de criptografia 3DES, AES 128, AES 256 e AESGCM16-256;

14.166.3. Suportar algoritmos Hash no mínimo SHA-1, SHA-256 e SHA-384;

14.166.4. Diffie-Hellman: Grupo 2 (1024 bits), Grupo 5 (1536 bits) e Grupo 14 (2048 bits);

14.166.5. Deverá suportar algoritmo Internet Key Exchange (IKE)v1 e v2;

14.166.6. Autenticação via de tuneis IPSec via certificado digital para VPNs Site-to-Site e Client-to-Site;

14.166.7. A solução deve suportar VPNs L2TP, incluindo suporte para Apple iOS e Android;

14.166.8. Solução deve suportar VPNs baseadas em políticas, e VPNs baseadas em roteamento estático e/ou dinâmico;

14.166.9. Suportar políticas de roteamento sobre conexões VPN IPSEC do tipo Site-to-Site com diferentes métricas e serviços. A rota poderá prover aos usuários diferentes caminhos redundantes sobre todas as conexões VPN IPSEC;

14.166.10. Solução deve incluir a capacidade de estabelecer VPNs com outros firewalls que utilizam IP públicos dinâmicos;

14.166.11. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do circuito primário;

14.166.12. Permitir criação de políticas de roteamento estático utilizando IPs de origem, destino, serviços e a própria VPN como parte encaminhadora deste tráfego, sendo este visto pela regra de roteamento como uma interface simples de rede para encaminhamento do tráfego;

14.166.13. Suportar a criação de túneis IP sobre IP (IPSEC Tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

14.166.14. Implementar os esquemas de troca de chaves manual, IKE e IKEv2 por Pré-Shared Key, certificados digitais e XAUTH client authentication;

14.166.15. Permitir a definição de um gateway redundante para terminação de VPN no caso de queda do primário;

14.166.16. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall.

14.167. ALTA DISPONIBILIDADE:

14.167.1. Devem ser fornecidos 02 (dois) appliances de NGFW com gerenciamento unificado, novos e sem uso anterior, funcionando em alta disponibilidade. O modelo ofertado deverá estar em linha de produção, sem previsão de encerramento de fabricação, na data de entrega da proposta. O software deverá ser fornecido em sua versão mais atualizada;

14.167.2. A solução deve ser entregue operando em alta disponibilidade no modo Ativo/Passivo, com as implementações de Failover;

14.167.3. Não serão permitidas soluções de cluster (HA) que façam com que os equipamentos se reiniciem após qualquer modificação de parâmetro/configuração realizada pelo administrador;

14.167.4. A solução deve ter capacidade de fazer monitoramento físico das interfaces dos membros do cluster;

14.167.5. A solução deve operar em alta disponibilidade implementando monitoramento lógico de um host na rede, e possibilitar failover;

14.167.6. A solução deve permitir o uso de endereço MAC virtual para evitar problemas de expiração de tabela ARP em caso de Failover;

14.167.7. A solução deve possibilitar a sincronização de todas as configurações realizadas na caixa principal do cluster incluído, mas não limitado a objetos, regras, rotas, VPNs e políticas de segurança;

14.167.8. A solução deve permitir visualizar no equipamento principal, o status da comunicação entre os parceiros do cluster, status de sincronização das configurações, status atual do equipamento redundante;

14.167.9. A solução de HA deve permitir que o dispositivo primário trate todo o tráfego, mantendo o dispositivo secundário atualizado em tempo real sobre as informações de conexão de rede, garantindo uma transição transparente para o dispositivo secundário em caso de failover, sem que haja perda das conexões de VPN, FTP, Oracle SQL*NET, Real Audio, VPN Client, Dynamic Arp Objects, Informações de DHCP Server, Multicast , IGMP, Usuários ativos, RIP e OSPF.

14.168. CONTROLE DE AMEAÇAS:

14.168.1. Para as ameaças de dia-zero, a solução deve ter a habilidade de prevenir o ataque antes de qualquer assinatura ser criada. Deve possuir módulo de Anti-Vírus e Anti-Bot integrado ao próprio appliance de segurança;

14.168.2. A solução deve possuir nuvem de inteligência proprietária do fabricante onde seja responsável em atualizar toda a base de segurança dos appliances através de assinaturas;

14.168.3. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e qualquer outro mecanismo de redirecionamento de tráfego;

14.168.4. Implementar funcionalidade de detecção e bloqueio de “call-backs”.

14.169. CARACTERISTICAS DE REDE:

14.169.1. A solução deverá ser capaz de detectar e bloquear comportamento suspeito ou anormal da rede;

14.169.2. A solução Anti-bot deve possuir mecanismo de detecção que inclua reputação de endereço IP;

14.169.3. Implementar interface gráfica WEB segura, utilizando o protocolo HTTPS;

14.169.4. Implementar interface CLI segura através do protocolo SSH;

14.169.5. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado à plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, IMAP, POP3, FTP, CIFS e TCP Stream;

14.169.6. A solução deve permitir criar regras de exceção de acordo com a proteção;

14.169.7. Deve possuir visualização na própria interface de gerenciamento referente aos top incidentes através de hosts, ou incidentes referentes a vírus e Bots;

14.169.8. Permitir o bloqueio de malwares (vírus, worms, spyware e etc);

14.169.9. A solução deve ser capaz de proteger contra ataques a DNS;

14.169.10. A solução deverá ser gerenciada a partir de uma console centralizada com políticas granulares;

14.169.11. A solução deve ser capaz de prevenir acesso a websites maliciosos;

14.169.12. A solução deve ser capaz de realizar inspeção de tráfego SSL/TLS e SSH;

14.169.13. A solução deverá receber atualizações de um serviço baseado em cloud;

14.169.14. A solução deverá ser capaz de bloquear a entrada de arquivos maliciosos;

14.169.15. A solução Anti-Vírus deverá suportar análise de arquivos que trafegam dentro do protocolo CIFS;

14.169.16. A solução deve suportar funcionalidade de Geo-IP, ou seja, a capacidade de identificar, isolar e controlar tráfego baseado na localização (origem e/ou destino), incluindo a capacidade de configuração de listas customizadas para esta mesma finalidade;

14.169.17. A solução de segurança deverá ter mecanismos de proteção de ameaças em tempo real pela análise de instruções e do uso da memória, sendo eficientes frente ameaças exploradas por vulnerabilidades do tipo meltdown;

14.169.18. A solução de Gateway AntiVirus deverá ter a tecnologia complementar de Anti Virus-Cloud, para que os mecanismos existentes de verificação sejam ampliados;

14.169.19. A solução deve bloquear proativamente o acesso a domínios maliciosos conehcidos por meio de filtragem DNS, reduzindo assim o risco de infecções por malware e outros ataques cibernéticos;

14.169.20. A solução deve prover o bloqueio de URL baseado em reputação, identificando e bloqueando proativamente entidades suspeitas.

14.170. PROTEÇÃO CONTRA ATAQUES AVANÇADOS:

14.170.1. A solução deverá prover as funcionalidades de inspeção de tráfego de entrada e saída de malwares não conhecidos ou do tipo APT, com filtro de ameaças avançadas e análise de execução em tempo real, e inspeção de tráfego de saída de “call-backs”;

14.170.2. Suportar os protocolos HTTP assim como inspeção de tráfego criptografado através de HTTPS;

14.170.3. A solução deve ser capaz de inspecionar o tráfego criptografado SSL/TLS e SSH;

14.170.4. Identificar e bloquear a existência de malware em comunicações de entrada e saída, incluindo destinos de servidores do tipo Comando e Controle;

14.170.5. Implementar mecanismo de bloqueio de vazamento não intencional de dados oriundos de máquinas existentes no ambiente LAN em tempo real;

14.170.6. Implementar detecção e bloqueio imediato de malwares que utilizem mecanismo de exploração em arquivos no formato PDF, sendo que a solução deve inspecionar arquivo PDF com até 10Mb;

14.170.7. Implementar a análise de arquivos maliciosos em ambiente controlado com, no mínimo, sistema operacional Windows e Android;

14.170.8. Conter ameaças de dia zero permitindo ao usuário final o recebimento dos arquivos livres de malware;

14.170.9. A tecnologia de máquina virtual deverá suportar diferentes sistemas operacionais, de modo a permitir a análise completa do comportamento do malware ou código malicioso sem utilização de assinaturas;

14.170.10. A solução deve possuir nuvem de inteligência proprietária do fabricante, onde este seja responsável por atualizar toda a base de segurança dos appliance através de assinaturas;

14.170.11. Implementar a visualização dos resultados das análises de malwares de dia zero nos diferentes sistemas operacionais dos ambientes controlados (sandbox) suportados;

14.170.12. Implementar modo de configuração totalmente transparente para o usuário final e usuários externos, sem a necessidade de configuração de proxies, rotas estáticas e quaisquer outros mecanismos de redirecionamento de tráfego;

14.170.13. Conter ameaças avançadas de dia zero;

14.170.14. Toda análise deverá ser realizada de forma automatizada sem a necessidade de criação de regras específicas e/ou interação de um operador;

14.170.15. Implementar mecanismo do tipo múltiplas fases para verificação de malware e/ou códigos maliciosos;

14.170.16. Toda a análise e bloqueio de malwares e/ou códigos maliciosos deve ocorrer em tempo real. Não serão aceitas soluções que apenas detectam o malware e/ou códigos maliciosos;

14.170.17. Suportar a análise de arquivos do pacote office (.doc, .docx, .xls, .xlsx, .ppt, .pptx) e Android APKs no ambiente controlado;

14.170.18. Implementar a análise de arquivos executáveis, DLLs e ZIP no ambiente controlado;

14.170.19. Possuir Anti-Vírus em tempo real, para ambiente de gateway internet integrado a plataforma de segurança para os seguintes protocolos: HTTP, HTTPS, SMTP, POP3, FTP, IMAP e CIFS;

14.170.20. Mitigar ameaças de dia zero de forma transparente para o usuário final;

14.170.21. Mitigar ameaças de dia zero através de tecnologias de emulação e código de registro;

14.170.22. Implementar mecanismo de pesquisa por diferentes intervalos de tempo;

14.170.23. Mitigar ameaças de dia zero via tráfego de internet;

14.170.24. Permitir a contenção de ameaças de dia zero sem a alteração da infra-estrutura de segurança;

14.170.25. Mitigar ameaças de dia zero que possam burlar o sistema operacional emulado;

14.170.26. A solução deve permitir a criação de listas brancas (whitelist) baseaas no MD5 do arquivo;

14.170.27. Mitigar ameaças de dia zero antes da execução e evasão de qualquer código malicioso;

14.170.28. Conter e mitigar exploits avançados;

14.170.29. A análise em nuvem ou local deve prover informações sobre as ações do malware na máquina infectada, informações sobre quais aplicações são utilizadas para causar/propagar a infecção, detectar aplicações não confiáveis utilizadas pelo malware, gerar assinaturas de Anti-Vírus e Anti-Spyware automaticamente, definir URLs não confiáveis utilizadas pelo novo malware e prover Informações sobre o usuário infectado (seu endereço IP e seu login de rede);

14.170.30. Suporte a submissão manual de arquivos para análise através do serviço de Sandbox;

14.170.31. As estratégias de análise, identificação e mitigação de ameaças devem também oferecer a capacidade de proteção contra ameaças que se alojam em memória, atuando permanentemente e em tempo real;

14.170.32. A Solução de segurança de FireWalls deverá ter um sistema de inspeção baseado em fluxo que execute análises simultâneas de tráfego de entrada e saída em alta velocidade, sem proxying or buffering;

14.170.33. A Solução deve unificar diversas funções de segurança em um único conjunto integrado, inspecionando os arquivos de usuários locais, remotos e móveis;

14.170.34. A Solução deve descriptografar e inspecionar o tráfego criptografado, como HTTPS, SMTPS, NNTPS, etc., sem afetar o desempenho;

14.170.35. A solução de segurança de Firewalls deverá fornecer tecnologias avançadas de proteção contra ameaças, com sandboxing usando multi-mecanismos baseado em nuvem, permitindo:

14.170.35.1. Inspeção profunda de memória em tempo real;

14.170.35.2. Inspeção profunda de pacotes livre de remontagem;

14.170.35.3. Descriptografia e inspeção TLS/SSL;

14.170.35.4. Inteligência e controle de aplicativos;

14.170.35.5. Recursos SD-WAN seguros.

14.170.36. É imprescindível que a solução não possua um limite de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a

entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

14.171. CARACTERÍSTICAS DE FILTRO DE CONTEÚDO WEB:

14.171.1. Possuir filtro de conteúdo integrado ao NGFW para classificação de páginas web com, no mínimo, 89 (oitenta e nove) categorias distintas, com mecanismo de atualização e consulta automáticas;

14.171.2. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs, através da integração com serviços de diretório, Active Directory e base de dados local;

14.171.3. Devem ser fornecidas licenças de filtro de conteúdo para cada equipamento e quantidade de usuários ilimitada, provendo atualização automática e em tempo real através da categorização contínua de novos sites da Internet, sem custo adicional, por todo o período de vigência da garantia e do contrato de manutenção e suporte técnico;

14.171.4. Permitir a customização de página de bloqueio;

14.171.5. Controle de conteúdo filtrado por categorias de sites com base de dados continuamente atualizada pelo fabricante;

14.171.6. Deve permitir submissão de novos sites para categorização;

14.171.7. Permitir a classificação dinâmica de sitesweb, URLs e domínios;

14.171.8. Permitir a associação de grupos de usuários a diferentes regras de filtragem de sites web, definindo quais categorias deverão ser bloqueadas ou permitidas para cada grupo de usuários, podendo ainda adicionar ou retirar acesso a domínios específicos da Internet;

14.171.9. Permitir a definição de quais zonas de segurança terão aplicadas as regras de filtragem de web;

14.171.10. Permitir aplicar a política de filtro de conteúdo baseada em horário do dia, bem como dia da semana.

14.172. CARACTERÍSTICAS DE AUTENTICAÇÃO:

14.172.1. Prover autenticação de usuários para os serviços Telnet, FTP, HTTP e HTTPS, utilizando as bases de dados de usuários e grupos de servidores Windows e Unix, de forma simultânea;

14.172.2. Permitir a autenticação dos usuários utilizando servidores LDAP, AD, RADIUS, Tacacs+, Single Sign On e API;

14.172.3. Permitir o cadastro manual dos usuários e grupos diretamente no NGFW por meio da interface de gerência remota do equipamento;

14.172.4. Permitir a integração com qualquer autoridade certificadora emissora de certificados X.509 que siga o padrão de PKI descrito na RFC 2459, inclusive verificando os certificados expirados/revogados, emitidos periodicamente pelas autoridades certificadoras, os quais devem ser obtidos automaticamente pelo NGFW;

14.172.5. Permitir o controle de acesso por usuário, para plataformas Microsoft Windows de forma transparente, para todos os serviços suportados, de forma que ao efetuar o logon na rede, um determinado usuário tenha seu perfil de acesso automaticamente configurado sem a instalação de softwares adicionais nas estações de trabalho e sem configuração adicional no browser;

14.172.6. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no NGFW;

14.172.7. Permitir aos usuários o uso de seu perfil independentemente do endereço IP da máquina que o usuário esteja utilizando;

14.172.8. Permitir a atribuição de perfil por faixa de endereço IP nos casos em que a autenticação não seja requerida;

14.172.9. Suportar a criação de túneis seguros sobre IP (IPSEC tunnel), de modo a possibilitar que duas redes com endereço inválido possam se comunicar através da Internet;

14.172.10. A solução deve possibilitar SSO via API;

14.172.11. O firewall deverá suportar autenticação SSO via SAML 2.0 (Security Assertion Markup Language) para integração com provedores de identidade em nuvem, garantindo compatibilidade com ao menos Azure AD/Entra ID, Google Workspace/G Suite e Okta;

14.172.12. A solução deve possuir funcionalidade de auditoria de credenciais (Credential Auditor), capaz de detectar e notificar sobre segredos ou senhas de firewalls gerenciados que sejam publicamente conhecidos, aumentando a postura de segurança dos ativos.

14.173. CARACTERÍSTICAS DE ADMINISTRAÇÃO E RELATÓRIOS:

14.173.1. Permitir a criação de perfis de administração distintos, de forma a possibilitar a definição de diversos administradores para o NGFW, cada um responsável por determinadas tarefas da administração;

14.173.2. Possuir mecanismo para aplicar remotamente, pela interface gráfica, correções e atualizações para o NGFW;

14.173.3. Possuir mecanismo para realizar remotamente, através de interface gráfica, cópias de segurança (backup) e restauração de configurações e sistema operacional;

14.173.4. Possuir mecanismo para agendamento realização das cópias de segurança(backups) de configuração;

14.173.5. Possuir mecanismo para exportar as configurações através de FTP, HTTPs ou SFTP;

14.173.6. A solução deve permitir ao administrador aplicar ajustes rápidos das melhores práticas de segurança no dispositivo com apenas um clique, possibilitando implementar as melhores práticas recomendadas pelo fabricante;

14.173.7. Permitir a visualização em tempo real de todas as conexões TCP e sessões UDP que se encontrem ativas através do NGFW e a remoção de qualquer uma destas sessões ou conexões;

14.173.8. Permitir a visualização, em forma gráfica, do percentual do uso de CPU e quantidade de tráfego de rede em todas as interfaces do NGFW em tempo real;

14.173.9. Permitir a visualização, em tempo real, dos serviços com maior tráfego e os endereços IP mais acessados;

14.173.10. Deve suportar minimamente dois tipos de negação de tráfego nas políticas de firewall: Descarte sem notificação do bloqueio ao usuário (discard), descarte com notificação do bloqueio ao usuário (drop), descarte com opção de envio de "ICMP Unreachable" para máquina de origem do tráfego, "TCP-Reset" para o cliente, "TCP-Reset" para o servidor ou para os dois lados da conexão;

14.173.11. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as aplicações mais utilizadas, os usuários que mais estão utilizando estes recursos informando sua sessão, total de pacotes enviados, total de bytes enviados e média de utilização em Kbps, URLs acessadas e ameaças identificadas;

14.173.12. Ser capaz de visualizar, de forma direta no appliance e em tempo real estado do processamento do produto e volume/desempenho de dados utilizado pela rede de computadores conectada ao equipamento;

14.173.13. Possibilitar a geração de relatório de ameaças com avaliação e gerenciamento de riscos e informações detalhadas sobre o ambiente, ajudando a identificar explorações de vulnerabilidades, intrusões e outras ameaças. Deve permitir a emissão deste relatório em formato PDF;

14.173.14. Ser capaz de visualizar, de forma direta no appliance e em tempo real, a largura de banda utilzida por política, por protocolo TCP/UDP IPV4 e IPV6;

14.173.15. Ser capaz de visualizar, de forma direta no appliance e em tempo real, as conexões estabelecidas, com possibilidade de aplicar filtros na visualização;

14.173.16. Possibilitar a geração de pelo menos os seguintes tipos de relatório, mostrados em formato HTML e CSV: máquinas mais acessadas, serviços mais utilizados, usuários que mais utilizaram serviços, URLs mais visualizadas, ou categorias Web mais acessadas (considerando a existência do filtro de conteúdo Web);

14.173.17. Permitir habilitar auditoria de configurações no equipamento, possibilitando o rastreio das configurações aplicadas no produto;

14.173.18. Ser capaz de implementar a funcionalidade de "Zero-Touch", permitindo que o equipamento se provisione autônoma e automaticamente no sistema de gestão centralizada;

14.173.19. A solução deve possuir mecanismo de gerenciamento através de aplicativo móvel, com disponibilidade para os sistemas operacionais IOS e Android;

14.173.20. O aplicativo móvel deve possibilitar conexão ao dispositivo via protocolo HTTPS e conexão USB;

14.173.21. O gerenciamento via aplicativo móvel deve permitir visualização de status de consumo de banda, CPU, conexões ativas dos dispositivos e topologia do NGFW;

14.173.22. O aplicativomóvel deve permitir visualização de status das ameaças observadas e bloqueadas pelas funcionalidades de segurança de NGFW;

14.173.23. O aplicativo móvel deve permitir visualização dos últimos logs gerados no NGFW;

14.173.24. O aplicativo móvel deve permitir diagnósticos simples na solução, como testes ICMP e verificação DNS;

14.173.25. O aplicativo móvel deve permitir configurar interfaces, objetos e políticas de acesso, além de exportar configurações;

14.173.26. A solução deve possibilitar ao administrador habilitar ou desabilitar as capacidades de auto-provisionamento da plataforma através de ponto central de gerenciamento;

14.173.27. Deve ser capaz de emitir relatório, mostrando a saúde do ambiente, agendado ou sob demanda, que liste informações de aplicações, risco, atividade WEB, análise de botnets, análise de malware, ameaças, países por tráfego, Arquivos compartilhados por aplicações, sessões e recomendações;

14.173.28. A solução deve suportar API como alternativa à interface de linha de comando (CLI), para configurar funções diversas;

14.173.29. Deve permitir que os administradores criem/recuperem/excluam listas de URLs ou endereços IP a serem bloqueados por meio de chamadas de API RESTful;

14.173.30. Os desempenhos apontados para cada modelo dos Firewalls devem ser comprovados por documento de domínio público do fabricante. A ausência de tais documentos comprobatórios reservará ao órgão o direito de aferir a performance dos equipamentos em bancada, assim como atendimento de todas as funcionalidades especificadas neste edital. Caso seja comprovado o não atendimento das especificações mínimas nos testes de bancada, o fornecedor será considerado inabilitado. Todos os custos oriundos do teste de bancada serão custeados pelo fornecedor/vendedor do certame;

14.173.31. É imprescindível que as soluçoes não possuam limited de tamanho de inspeção de arquivos no uso da tecnologia 'gateway antimalware', já que tal restrição poderia permitir a entrega de arquivos a um usuário final sem qualquer tipo de análise, aumentando significativamente o risco de infecção no ambiente.

Equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo I com setup/implantação e suporte de 12 meses

14.174. REQUISITOS MÍNIMOS:

14.174.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 1 Gbps ou superior;

14.174.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 430 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

14.174.3. Desempenho mínimo de 1.5 Gbps de IPS;

14.174.4. Suporte mínimo de 1.000.000 conexões simultâneas/concorrentes em modo SPI;

14.174.5. Suporte mínimo de 12.000 novas conexões por segundo;

14.174.6. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

14.174.7. Deve possuir 8 interfaces 1 GbE padrão RJ-45 e possuir 2 interfaces SFP 1 GbE;

14.174.8. Deve possuir 1 interface do tipo console ou similar;

14.174.9. Deve possuir 1 interface USB-A ou USB-C;

14.174.10. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuário simultâneo. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos;

14.174.11. A VPN SSL deve ser licenciada para, no mínimo, 1 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 50 usuários simultâneos;

14.174.12. Deve suportar 200 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

14.174.13. Deve suportar, no mínimo, 1.2 Gbps de desempenho de VPN IPSEC;

14.174.14. O Equipamento deverá ser homologado pela ANATEL;

14.174.15. Não serão aceitas cartas ou declarações de fabricantes para atendimento aos valores de desempenho solicitados;

14.174.16. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no mínimo 12 meses;

14.174.17. A garantia do hardware deverá ser de 12 meses.

Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo II com setup/implantação e suporte de 12 meses

14.175. REQUISITOS MÍNIMOS:

14.175.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 1.5 Gbps ou superior;

14.175.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 600 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

14.175.3. Desempenho mínimo de 2 Gbps de IPS;

14.175.4. Suporte mínimo de 1.100.000 conexões simultâneas/concorrentes em modo SPI;

14.175.5. Suporte mínimo de 15.000 novas conexões por segundo;

14.175.6. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

14.175.7. Deve, obrigatoriamente, possuir suporte a redundância de alimentação elétrica por meio de fonte de alimentação adicional (interna ou externa);

14.175.8. Deve possuir 8 interfaces 1 GbE padrão RJ-45 e possuir 2 interfaces SFP+ 5 GbE;

14.175.9. Deve possuir 1 interface do tipo console ou similar;

14.175.10. Deve possuir 1 interface USB-A ou USB-C;

14.175.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 5 usuários simultâneo. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos;

14.175.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 100 usuários simultâneos;

14.175.13. Deve suportar 200 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

14.175.14. Deve suportar, no mínimo, 1.6 Gbps de desempenho de VPN IPSEC;

14.175.15. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no minimo 12 meses;

14.175.16. A garantia do hardware deverá ser de 12 meses.

Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo III com setup/implantação e suporte de 12 meses

14.176. REQUISITOS MÍNIMOS:

14.176.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 2.2 Gbps ou superior;

14.176.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 750 Mbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

14.176.3. Desempenho mínimo de 2.5 Gbps de IPS;

14.176.4. Suporte mínimo de 1.400.000 conexões simultâneas/concorrentes em modo SPI;

14.176.5. Suporte mínimo de 20.000 novas conexões por segundo;

14.176.6. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

14.176.7. Deve, obrigatoriamente, possuir suporte a redundância de alimentação elétrica por meio de fonte de alimentação adicional (interna ou externa);

14.176.8. Deve possuir 8 interfaces 1 GbE padrão RJ-45 e possuir 2 interfaces SFP+ 10 GbE;

14.176.9. Deve possuir 1 interface do tipo console ou similar;

14.176.10. Deve possuir 1 interface USB-A ou USB-C;

14.176.11. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 10 usuário simultâneo. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos;

14.176.12. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 200 usuários simultâneos;

14.176.13. Deve suportar 250 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

14.176.14. Deve suportar, no mínimo, 2.2 Gbps de desempenho de VPN IPSEC.

Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo IV com setup/implantação e suporte de 12 meses

14.177. REQUISITOS MÍNIMOS:

14.177.1. Desempenho em modo Threat Prevention (Proteção Anti-Malware, IPS e Controle de Aplicação habilitados) mínimo de 6 Gbps ou superior. Equipamento físico novo e original;

14.177.2. Desempenho em modo de Inspeção (decriptografia e criptografia) de tráfego criptografado (SSL/TLS) mínimo de 1.8 Gbps. Os desempenhos solicitados devem ser comprovados por documento de domínio público do fabricante. Não serão aceitas declarações ou cartas de fabricantes para atendimento deste item;

14.177.3. Desempenho mínimo de 7 Gbps de IPS;

14.177.4. Suporte mínimo de 2.000.000 conexões simultâneas/concorrentes no modo SPI;

14.177.5. Suporte mínimo de 50.000 novas conexões por segundo;

14.177.6. Deve possuir armazenamento interno de no minimo 128 GB e suportar expansão de armazenamento interno para até 512Gb;

14.177.7. Deve possuir fonte de alimentação com chaveamento automático de 100-240 VAC;

14.177.8. Deve, obrigatoriamente, possuir redundância de alimentação elétrica por meio de fonte de alimentação adicional (interna ou externa);

14.177.9. Deve possuir 16 interfaces 1 GbE padrão RJ-45;

14.177.10. Deve possuir 3 interfaces 10GbE SFP+;

14.177.11. Deve possuir 1interface do tipo 1 GbE RJ-45 dedicada para gerenciamento do equipamento;

14.177.12. Deve possuir 2 interface USB 3.0 com suporte a tecnologias LTE 3G/4G e 5G;

14.177.13. A VPN Client-to-Site IPsec deve ser licenciada para, no mínimo, 50 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 1000 usuários simultâneos;

14.177.14. A VPN SSL deve ser licenciada para, no mínimo, 2 usuários simultâneos. O mesmo equipamento deverá suportar crescimento futuro para, no mínimo, 500 usuários simultâneos;

14.177.15. Deve suportar 2000 túneis de VPN tipo Site-to-Site padrão IPSEC simultâneos;

14.177.16. Deve suportar, no mínimo, 5.5Gbps de desempenho de VPN IPSEC;

14.177.17. O licenciamento para todos os serviços de Next Generation Firewall deverá ser de no minimo 12 meses;

14.177.18. A garantia do hardware deverá ser de 12 meses.

Solução Integrada de Proteção e Anonimização de Dados Pessoais em Documentos Digitais, contemplando plataforma tecnológica com inteligência artificial multimodal, criptografia pós-quântica e marca d'água invisível rastreável

14.178. A solução deverá operar como camada de proteção multiplataforma, integrando-se aos diversos sistemas e repositórios documentais do Estado do Rio de Janeiro mediante duas modalidades de conexão:

14.178.1. ONECTORES NATIVOS (fornecidos prontos pela solução):

14.178.1.1. SEI (Sistema Eletrônico de Informações): Integração via proxy reverso no servidor do SEI, interceptando visualização de processos sem alteração de código-fonte, processando documentos internos (HTML) e anexos externos (PDF, imagens, etc.);

14.178.1.2. NextCloud: Conector compatível com arquitetura de plugins NextCloud, permitindo anonimização transparente de documentos armazenados;

14.178.1.3. Google Drive: Conector nativo via Google Drive API v3, com suporte a OAuth 2.0 para autenticação;

14.178.1.4. Microsoft OneDrive: Conector nativo via Microsoft Graph API, com suporte a autenticação Azure AD.

14.178.2. API REST ABERTA (para integração por sistemas externos):

14.178.2.1. API RESTful documentada (OpenAPI 3.0/Swagger) que permite a qualquer sistema externo — SIGRH, ERPs estaduais, sistemas setoriais (SEEDUC, DEGASE, SEASDH, SEFAZ), ou qualquer outra aplicação — enviar documentos para anonimização, receber versões processadas e consultar status de processamento;

14.178.2.2. A integração via API é realizada pelo técnico responsável pelo sistema legado, utilizando a documentação fornecida pela solução;

14.178.2.3. Suporte a autenticação via OAuth 2.0, API Keys e integração com LDAP/AD;

14.178.2.4. Webhooks para notificação assíncrona de conclusão de processamento;

14.178.2.5. A solução a ser contratada deverá processar documentos digitais em múltiplos formatos, identificando automaticamente dados pessoais sensíveis mediante técnicas de inteligência artificial multimodal (processamento simultâneo de texto, imagem, áudio e vídeo), aplicando técnicas de anonimização conforme o contexto, perfil do usuário e finalidade do tratamento, garantindo a proteção da privacidade dos titulares dos dados sem comprometer a utilidade das informações

para fins administrativos, estatísticos, de transparência pública e de pesquisa científica ou histórica;

14.178.2.6. A solução de Proteção e Anonimização de Dados Pessoais em Documentos Digitais compreende plataforma tecnológica integrada e serviços técnicos especializados, organizados em cinco itens complementares que, em conjunto, proporcionam capacidade completa de tratamento de dados pessoais em conformidade com a legislação aplicável;

14.178.2.7. A arquitetura da solução devera operar como CAMADA DE PROTEÇÃO MULTIPLATAFORMA, interceptando solicitações de acesso a documentos em múltiplos sistemas e aplicando anonimização em tempo real conforme perfil do usuário e finalidade declarada. O documento original permanece intacto e cifrado no repositório de origem, atendendo simultaneamente às exigências da LGPD (minimização), LAI (transparência) e CONARQ (autenticidade);

14.178.2.8. A solução de Proteção e Anonimização de Dados Pessoais em Documentos Digitais devera ser uma plataforma tecnológica integrada e serviços técnicos especializados, organizados em cinco itens complementares que, em conjunto, proporcionam capacidade completa de tratamento de dados pessoais em conformidade com a legislação aplicável;

14.178.2.9. A arquitetura da solução devera operar como CAMADA DE PROTEÇÃO MULTIPLATAFORMA, interceptando solicitações de acesso a documentos em múltiplos sistemas e aplicando anonimização em tempo real conforme perfil do usuário e finalidade declarada. O documento original permanece intacto e cifrado no repositório de origem, atendendo simultaneamente às exigências da LGPD (minimização), LAI (transparência) e CONARQ (autenticidade).

14.178.3. Modelo de licenciamento e garantia:

14.178.3.1. A solução poderá ser disponibilizada em ambiente de infraestrutura própria do CONTRATANTE (on-premises) ou em ambiente de nuvem computacional gerenciado pela CONTRATADA (Full Cloud), com certificação de segurança adequada ao tratamento de dados pessoais e dados pessoais sensíveis;

14.178.3.2. O órgão aderente optará por Item I (On-Premise) OU Item II (Full Cloud), conforme sua infraestrutura e requisitos de segurança.

14.178.4. Os requisitos de negócio representam as necessidades organizacionais que motivam a contratação e que devem ser Requisitos de negócio, atendidas pela solução:

14.178.4.1. Possibilitar a anonimização automatizada de dados pessoais em documentos digitais, reduzindo o tempo de processamento de dias/semanas para minutos/horas;

14.178.4.2. Garantir conformidade com a Lei Geral de Proteção de Dados (Lei 13.709/2018), especialmente no que tange às obrigações de segurança e minimização de dados;

14.178.4.3. Assegurar proteção especial aos dados de crianças e adolescentes, em atendimento ao Estatuto da Criança e do Adolescente (Lei 8.069/1990) e ao ECA Digital (Lei 15.211/2025);

14.178.4.4. Viabilizar o atendimento tempestivo aos pedidos de acesso à informação (Lei 12.527/2011) que envolvam documentos com dados pessoais;

14.178.4.5. Permitir a disponibilização de documentos em portais de transparência com proteção adequada aos dados pessoais;

14.178.4.6. Proporcionar rastreabilidade completa das operações de anonimização para fins de auditoria e prestação de contas;

14.178.4.7. Padronizar os procedimentos de anonimização em toda a Administração Estadual, assegurando tratamento uniforme aos dados pessoais;

14.178.4.8. Capacitar servidores públicos em proteção de dados pessoais e uso da plataforma;

14.178.4.9. Integrar-se aos sistemas de gestão documental existentes, especialmente o SEI, minimizando mudanças nos fluxos de trabalho.

14.178.5. Requisitos de funcionais:

14.178.5.1. A plataforma de anonimização deverá atender aos seguintes requisitos funcionais:

14.178.5.1.1. Quanto ao processamento de documentos:

14.178.5.1.1.1. Processar documentos nos formatos PDF (nativo e digitalizado), imagens (JPEG, PNG, TIFF, BMP), documentos de texto (DOC, DOCX, ODT, TXT), planilhas (XLS, XLSX, ODS, CSV), apresentações (PPT, PPTX, ODP), e-mails (EML, MSG) e arquivos compactados (ZIP, RAR, 7Z);

14.178.5.1.1.2. Possuir capacidade de reconhecer e processar dados pessoais em documentos digitais, manuscritos e digitalizados, com suporte ao idioma português do Brasil e taxa de acurácia mínima de 98%;

14.178.5.1.1.3. Processar documentos de áudio nos formatos MP3, WAV, OGG, M4A e FLAC, com transcrição automática e identificação de dados pessoais na fala;

14.178.5.1.1.4. Processar documentos de vídeo nos formatos MP4, AVI, MOV, MKV e WMV, com identificação de dados pessoais tanto na trilha de áudio quanto nas imagens (rostos, documentos, placas);

14.178.5.1.1.5. Suportar o processamento em lote de múltiplos documentos simultaneamente, com capacidade mínima de 10.000 páginas por hora em operação regular;

14.178.5.1.1.6. Permitir a definição de prioridades de processamento para atendimento a demandas urgentes.

14.178.5.1.2. Quanto à identificação de dados pessoais:

14.178.5.1.2.1. Identificar automaticamente as seguintes categorias de dados pessoais: nome completo, CPF, RG, data de nascimento, endereço completo, telefone, e-mail, dados bancários, número de matrícula, nome de mãe/pai, naturalidade, nacionalidade, estado civil, profissão, local de trabalho, assinatura manuscrita e digital;

14.178.5.1.2.2. Identificar dados pessoais sensíveis: origem racial ou étnica, convicção religiosa, opinião política, filiação sindical ou partidária, dados de saúde (CID, procedimentos, medicamentos, laudos), dados biométricos, dados genéticos e vida sexual;

14.178.5.1.2.3. Identificar dados específicos de menores de idade: nome, filiação, escola, série/turma, registro de ocorrência, medida socioeducativa, conselho tutelar, vara da infância;

14.178.5.1.2.4. Detectar rostos humanos em imagens e vídeos para aplicação de anonimização facial;

14.178.5.1.2.5. Identificar documentos de identificação (RG, CNH, passaporte, carteira funcional) em imagens, com extração e anonimização dos dados neles contidos;

14.178.5.1.2.6. Permitir a definição de regras customizadas para identificação de dados específicos do contexto do órgão.

14.178.5.1.3. Quanto às técnicas de anonimização:

14.178.5.1.3.1. Aplicar técnica de SUPRESSÃO/REDAÇÃO em documentos de texto, removendo completamente o dado pessoal e inserindo marcador indicativo (ex.: [SUPRIMIDO], [REDACTED] ou equivalente);

14.178.5.1.3.2. Aplicar técnica de TARJAMENTO em documentos de imagem, sobrepondo bloco opaco (tarja preta ou colorida) sobre o dado pessoal identificado, tornando-o visualmente ilegível;

14.178.5.1.3.3. Aplicar desfoque (blur) em rostos e elementos visuais identificadores em imagens e vídeos;

14.178.5.1.3.4. Aplicar distorção ou supressão de voz em arquivos de áudio e trilhas de vídeo contendo dados pessoais verbalizados;

14.178.5.1.3.5. Permitir a configuração de diferentes níveis de proteção para diferentes categorias de dados, conforme política definida pelo DPO.

14.178.5.1.3.5.1. A solução NÃO utilizará técnicas de generalização (ex.: idade por faixa etária) nem pseudonimização reversível (substituição por tokens). O método adotado é exclusivamente SUPRESSÃO TOTAL,

garantindo que o dado pessoal seja completamente removido da visualização, sem possibilidade de reidentificação por terceiros.

14.178.5.1.4. Quanto à interface de usuário:

14.178.5.1.4.1. Disponibilizar interface web responsiva, compatível com os navegadores Chrome, Firefox, Edge e Safari em suas versões atuais e duas anteriores;

14.178.5.1.4.2. Permitir upload de documentos mediante drag-and-drop, seleção de arquivos ou indicação de URL;

14.178.5.1.4.3. Exibir visualização comparativa antes/depois da anonimização, com destaque para os dados identificados e as técnicas aplicadas;

14.178.5.1.4.4. Permitir revisão e ajuste manual dos resultados da anonimização automática antes da confirmação;

14.178.5.1.4.5. Disponibilizar dashboard com estatísticas de uso, volumes processados, tipos de dados identificados e indicadores de qualidade;

14.178.5.1.4.6. Atender aos requisitos de acessibilidade digital conforme WCAG 2.1 nível AA e e-MAG 3.1.

14.178.5.1.5. Quanto aos CONECTORES NATIVOS (fornecidos prontos pela solução):

14.178.5.1.5.1. Fornecer conector nativo para SEI (Sistema Eletrônico de Informações) via proxy reverso no servidor, interceptando visualização de processos sem alteração do código-fonte do sistema, processando documentos internos (HTML) e anexos externos;

14.178.5.1.5.2. Fornecer conector nativo para NextCloud, compatível com arquitetura de plugins do sistema, permitindo anonimização transparente de documentos armazenados com aplicação automática de políticas conforme diretório ou metadados;

14.178.5.1.5.3. Fornecer conector nativo para Google Drive via Google Drive API v3, com suporte a OAuth 2.0 para autenticação e autorização granular, permitindo anonimização no momento do acesso ou download de documentos;

14.178.5.1.5.4. Fornecer conector nativo para Microsoft OneDrive via Microsoft Graph API, com suporte a autenticação Azure AD, permitindo aplicação de políticas de anonimização por diretório, usuário ou grupo;

14.178.5.1.5.5. Garantir que os conectores operem de forma transparente, sem alterar o fluxo de trabalho do usuário — a anonimização deve ser aplicada automaticamente no momento do acesso, conforme matriz de visibilidade configurada pelo DPO;

14.178.5.1.5.6. Suportar anonimização tanto no fluxo de download (usuário solicita documento e recebe versão anonimizada) quanto no fluxo de visualização

online (documento exibido diretamente no navegador já com anonimização aplicada).

14.178.5.1.6. Quanto à API REST ABERTA (para integração por sistemas externos):

14.178.5.1.6.1. Disponibilizar API RESTful documentada (OpenAPI 3.0/Swagger) que permita a qualquer sistema externo — SIGRH, ERPs, sistemas setoriais ou qualquer outra aplicação — enviar documentos para anonimização e receber versões processadas;

14.178.5.1.6.2. A integração via API deve ser realizável pelo técnico responsável pelo sistema legado, utilizando apenas a documentação fornecida, sem necessidade de suporte especializado da CONTRATADA;

14.178.5.1.6.3. Suportar envio de documento via upload (multipart/form-data) ou codificação base64;

14.178.5.1.6.4. Suportar consulta de status de processamento (operação síncrona e assíncrona);

14.178.5.1.6.5. Disponibilizar webhooks para notificação assíncrona de conclusão de processamento;

14.178.5.1.6.6. Suportar autenticação via OAuth 2.0, API Keys e integração com LDAP/Active Directory;

14.178.5.1.6.7. Suportar Single Sign-On (SSO) via Gov.br e demais provedores de identidade utilizados pelo órgão;

14.178.5.1.6.8. Disponibilizar SDKs ou bibliotecas cliente para linguagens populares (Python, Java, JavaScript/TypeScript, C#).

14.178.5.1.7. Quanto à aplicação consistente de políticas multiplataforma:

14.178.5.1.7.1. Garantir que um mesmo documento, acessado via SEI, NextCloud, Google Drive, OneDrive ou qualquer outro sistema integrado, receba anonimização CONSISTENTE conforme o perfil do usuário solicitante;

14.178.5.1.7.2. Permitir que o DPO configure matriz de visibilidade UMA ÚNICA VEZ no Console DPO e que esta configuração seja aplicada automaticamente em TODOS os canais de acesso integrados;

14.178.5.1.7.3. Registrar em log unificado todas as operações de anonimização, independente do canal de origem, permitindo rastreabilidade completa e consolidada;

14.178.5.1.7.4. Aplicar watermark invisível em TODA visualização, independente do sistema de origem, garantindo rastreabilidade de vazamentos multiplataforma;

14.178.5.1.7.5. Suportar sincronização de perfis de usuário entre diferentes sistemas integrados, evitando necessidade de configuração duplicada.

14.178.6. A solução deverá atender aos seguintes requisitos tecnológicos:

14.178.6.1. Quanto à arquitetura:

14.178.6.1.1. Arquitetura baseada em microserviços, permitindo escalabilidade horizontal independente para cada componente;

14.178.6.1.2. Hospedagem em ambiente de ambiente computacional seguro com certificações de segurança (ISO 27001, SOC 2 Tipo II);

14.178.6.1.3. Data centers localizados exclusivamente em território brasileiro;

14.178.6.1.4. Redundância geográfica com replicação de dados em pelo menos duas localidades;

14.178.6.1.5. Capacidade de processamento escalável conforme demanda, sem degradação perceptível de performance.

14.178.6.2. Quanto à segurança:

14.178.6.2.1. Criptografia de dados em trânsito mediante TLS 1.3 ou superior;

14.178.6.2.2. Criptografia de dados em repouso mediante AES-256 ou algoritmo pós-quântico equivalente;

14.178.6.2.3. Autenticação multifator (MFA) obrigatória para acesso administrativo;

14.178.6.2.4. Integração com provedores de identidade mediante SAML 2.0 ou OpenID Connect;

14.178.6.2.5. Segregação lógica de dados entre diferentes órgãos (multi-tenancy seguro);

14.178.6.2.6. Registro de auditoria (logs) de todas as operações, com retenção mínima de 5 (cinco) anos;

14.178.6.2.7. Testes de penetração (pentest) anuais, com relatório disponibilizado ao CONTRATANTE.

14.178.6.3. Quanto aos CONECTORES NATIVOS:

14.178.6.3.1. Conector nativo para SEI (Sistema Eletrônico de Informações) via proxy reverso, sem alteração de código-fonte;

14.178.6.3.2. Conector nativo para NextCloud compatível com arquitetura de plugins, permitindo anonimização transparente no momento do acesso;

14.178.6.3.3. Conector nativo para Google Drive via Google Drive API v3, com suporte a OAuth 2.0 e autorização granular por pasta/documento;

14.178.6.3.4. Conector nativo para Microsoft OneDrive via Microsoft Graph API, com suporte a autenticação Azure AD.

14.178.6.4. Quanto à API REST ABERTA (para sistemas externos:

14.178.6.4.1. Disponibilização de API RESTful documentada (OpenAPI 3.0/Swagger) que permita a qualquer sistema externo (SIGRH, ERPs, sistemas setoriais, etc.) integrar-se para envio e recebimento de documentos anonimizados;

14.178.6.4.2. Suporte a autenticação via OAuth 2.0, SAML 2.0 e API Keys para acesso programático;

14.178.6.4.3. Suporte a webhooks para notificação assíncrona de conclusão de processamento;

14.178.6.4.4. Disponibilização de SDK ou bibliotecas cliente para linguagens de programação populares (Python, Java, JavaScript/TypeScript, C#);

14.178.6.4.5. Documentação técnica suficiente para que o técnico do sistema legado realize a integração sem suporte especializado da CONTRATADA.

14.178.6.5. Quanto à integração com HSM:

14.178.6.5.1. Suporte a integração com HSM (Hardware Security Module) externo via protocolo PKCS#11 ou API REST para custódia de chaves criptográficas;

14.178.6.5.2. Compatibilidade com HSM Thales CipherTrust (já implantado no Estado) para aproveitamento de investimento existente;

14.178.6.5.3. Possibilidade de custodiar chaves de criptografia pós-quântica, chaves de geração de watermarks forenses e chaves de assinatura de logs de auditoria no HSM externo;

14.178.6.5.4. Capacidade de operação autônoma (sem HSM externo) quando o órgão não dispuser de infraestrutura de HSM.

Licença Perpétua: Plataforma On-Premise

14.179. Compreende a aquisição de licença perpétua de uso de plataforma tecnológica especializada em identificação, classificação e anonimização de dados pessoais em documentos digitais, na modalidade ON-PREMISE, com processamento realizado integralmente em infraestrutura própria do CONTRATANTE, incluindo garantia técnica de 12 (doze) meses;

14.180. ARQUITETURA DA MODALIDADE ON-PREMISE:

14.180.1. A solução opera em modelo híbrido, com separação entre governança (nuvem) e processamento (local):

14.180.1.1. CONSOLE DPO (nuvem da CONTRATADA): Interface web hospedada na infraestrutura da CONTRATADA, onde o Encarregado (DPO) configura políticas de anonimização, matriz de visibilidade, grupos de usuários e regras de negócio. O Console NÃO processa nem armazena documentos ou dados pessoais — apenas regras e configurações;

14.180.1.2. BANCO DE REGRAS LOCAL (infra do CONTRATANTE): Banco de dados instalado na infraestrutura do CONTRATANTE que sincroniza as regras definidas no Console DPO. Permite operação offline após sincronização inicial;

14.180.1.3. SERVIÇO DE TARJAMENTO (infra do CONTRATANTE): Motor de processamento instalado na infraestrutura do CONTRATANTE que consome as regras do banco local e executa a anonimização. Documentos são processados localmente e NUNCA são transmitidos para a nuvem da CONTRATADA;

14.180.1.4. CONECTORES (infra do CONTRATANTE): Instalados na infraestrutura do CONTRATANTE, integram-se ao SEI, NextCloud e demais sistemas, direcionando documentos ao serviço de tarjamento local.

14.181. GARANTIA DE NÃO RETENÇÃO DE DADOS:

14.181.1. A CONTRATADA NÃO armazena documentos processados, dados pessoais ou dados sensíveis em nenhum momento;

14.181.2. O Console DPO armazena APENAS regras de negócio, configurações e logs de auditoria (sem conteúdo de documentos).

14.182. ENTREGÁVEIS DO ITEM:

14.182.1. 1. PACOTE DE INSTALAÇÃO (para infraestrutura do CONTRATANTE):

14.182.1.1. Imagens de container (Docker/Podman) ou pacotes para Linux (Ubuntu 20.04+, RHEL 8+, Debian 11+);

14.182.1.2. Modelos de IA embarcados para operação offline;

14.182.1.3. Scripts de instalação e health-check.

14.182.2. 2. SERVIÇO DE TARJAMENTO com módulos:

14.182.2.1. Anonimização por IA Multimodal (texto, imagem, áudio, vídeo);

14.182.2.2. Criptografia Pós-Quântica (ML-KEM-768/FIPS 203);

14.182.2.3. Watermark Forense (resistente a print-scan).

14.182.3. 3. ACESSO AO CONSOLE DPO (interface web na nuvem da CONTRATADA):

14.182.3.1. Configuração de políticas de anonimização e matriz de visibilidade;

14.182.3.2. Gerenciamento de grupos (manual e LDAP/AD);

14.182.3.3. Dashboards, relatórios e ferramenta de análise forense.

14.182.4. 4. CONECTORES NATIVOS:

14.182.4.1. Conector SEI — proxy reverso, sem alteração de código-fonte;

14.182.4.2. Conector NextCloud — plugin nativo;

14.182.4.3. Conector Microsoft OneDrive — via Microsoft Graph API.

14.182.5. 5. API REST ABERTA:

14.182.5.1. API documentada (OpenAPI 3.0) para integração de sistemas externos (SIGRH, ERPs, etc.);

14.182.5.2. SDKs, webhooks e autenticação OAuth 2.0/API Keys/LDAP.

Licença Perpétua: Plataforma Plataforma Full Cloud

14.183. Compreende a aquisição de licença perpétua de uso de plataforma tecnológica especializada em identificação, classificação e anonimização de dados pessoais em documentos digitais, na modalidade FULL

CLOUD, com processamento realizado integralmente na infraestrutura de nuvem da CONTRATADA, incluindo garantia técnica de 12 (doze) meses;

14.184. ARQUITETURA DA MODALIDADE FULL CLOUD:

14.184.1. A solução opera integralmente na nuvem da CONTRATADA, sem necessidade de infraestrutura local:

14.184.1.1. CONSOLE DPO (nuvem da CONTRATADA): Interface web onde o Encarregado (DPO) configura políticas de anonimização, matriz de visibilidade, grupos de usuários e regras de negócio;

14.184.1.2. SERVIÇO DE TARJAMENTO (nuvem da CONTRATADA): Motor de processamento que executa a anonimização. Documentos são enviados, processados e retornados ao CONTRATANTE em tempo real;

14.184.1.3. CONECTORES (nuvem da CONTRATADA): Integram-se remotamente ao SEI, NextCloud e demais sistemas do CONTRATANTE.

14.185. GARANTIA DE NÃO RETENÇÃO DE DADOS:

14.185.1. A CONTRATADA NÃO armazena documentos processados, dados pessoais ou dados sensíveis em nenhum momento;

14.185.2. O processamento ocorre em memória (streaming) — documento entra, é processado e retorna ao CONTRATANTE imediatamente;

14.185.3. Apenas logs de auditoria (metadados, sem conteúdo) e configurações são armazenados.

14.186. ENTREGÁVEIS DO ITEM:

14.186.1. 1. ACESSO AO CONSOLE DPO (interface web):

14.186.1.1. Configuração de políticas de anonimização e matriz de visibilidade;

14.186.1.2. Gerenciamento de grupos (manual e LDAP/AD);

14.186.1.3. Dashboards, relatórios e ferramenta de análise forense.

14.186.2. 2. SERVIÇO DE TARJAMENTO CLOUD com módulos:

14.186.2.1. Anonimização por IA Multimodal (texto, imagem, áudio, vídeo);

14.186.2.2. Criptografia Pós-Quântica (ML-KEM-768/FIPS 203);

14.186.2.3. Watermark Forense (resistente a print-scan).

14.186.3. 3. CONECTORES NATIVOS (operando na nuvem):

14.186.3.1. Conector SEI — integração remota via API;

14.186.3.2. Conector NextCloud — integração remota;

14.186.3.3. Conector Google Drive — via Google Drive API v3;

14.186.3.4. Conector Microsoft OneDrive — via Microsoft Graph API.

14.186.4. 4. API REST ABERTA:

14.186.4.1. API documentada (OpenAPI 3.0) para integração de sistemas externos;

14.186.4.2. SDKs, webhooks e autenticação OAuth 2.0/API Keys/LDAP.

Créditos de Processamento para Anonimização de Documentos

14.187. Compreende a aquisição de créditos de processamento para anonimização de documentos digitais. Cada crédito corresponde ao processamento de 1 (uma) página A4 equivalente, conforme métrica definida na seção de Métricas de Aferição e Pagamento;

14.188. Os créditos de processamento serão consumidos conforme o volume de documentos submetidos à plataforma para anonimização, independentemente da modalidade de licenciamento contratada (On-Premise ou Full Cloud);

14.189. O dimensionamento dos créditos considera:

14.189.1. Volume estimado do acervo documental dos órgãos participantes;

14.189.2. Projeção de crescimento vegetativo do acervo durante a vigência da Ata;

14.189.3. Margem de segurança para atendimento a demandas não previstas.

14.190. A página equivalente é calculada conforme os seguintes fatores de conversão:

14.190.1. Documentos textuais: 2.100 caracteres = 1 Página Equivalente;

14.190.2. Documentos de imagem: Número de páginas × Fator de tamanho (A4=1,0; A3=2,0; A2=4,0; A1=8,0; A0=16,0).

SERVIÇO DE SETUP E IMPLANTAÇÃO - RELATIVOS A TODOS OS ITENS DESTE TERMO DE REFERÊNCIA

14.191. O serviço de Setup e Implantação tem como objetivo assegurar a configuração correta, a integração e a entrada em operação de todas as camadas da solução de segurança da informação descrita neste Termo de Referência para:

14.191.1. Plataforma unificada de segurança cibernética para proteção integrada de endpoints, proteção de e-mail, nuvem, identidade, rede, dados, campanha de pishing, EDR, DLP e usuários com automação inteligente;

14.191.2. Soluçao de End Point Response – EDR;

14.191.3. Solução de Proteção e Prevenção de Vazamento de Dados (DLP);

14.191.4. Software de SIEM -Security Information&Event Management;

14.191.5. Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos, conformidade, maturidade;

14.191.6. Sistema de Backup Resilente, recuperação via DR Online;

14.191.7. SOC - Security Operations Center – 24x7, 365 dias por ano;

14.191.8. Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM) anti-ransomware;

14.191.9. Soluçao de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados;

14.191.10. Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação;

14.191.11. Soluçoes de Firewall Next Generation.

14.192. Todas as soluções mencionadas neste Termo de Referência deverão obrigatoriamente incluir, em seus valores propostos, o processo completo de setup e implantação, não sendo admitidos custos adicionais posteriores para essas atividades. Para isso, a PROPONENTE deverá apresentar no inicio do projeto um cronograma de atividade a serem a serem executadas de forma planejada e controlada, de modo a garantir que cada componente seja implantado de forma coordenada e alinhada aos requisitos técnicos, normativos e de negócio da CONTRATANTE;

14.193. Os treinamentos incluídos nos serviços de operação assistida deverão ser definidos e planejados conjuntamente entre a CONTRATANTE e a CONTRATADA na fase inicial do projeto, visando à elaboração de um cronograma detalhado. Esse cronograma deverá contemplar, no mínimo, os públicos-alvo, conteúdos programáticos, cargas horárias, formatos (presencial ou remoto), periodicidade, pré-requisitos e critérios de participação, de modo a assegurar a adequada capacitação das equipes envolvidas e a plena utilização das soluções contratadas;

14.194. O objetivo central do serviço é transformar o conjunto de soluções contratadas em uma plataforma integrada de defesa em profundidade contra ataques de segurança da informação e entregar as soluções plenamente operacionais e aderentes às melhores práticas de gestão de mercado, devendo para isso:

14.194.1. Configurar todas as soluções em conformidade com o desenho arquitetural aprovado;

14.194.2. Parametrizar regras, políticas e integrações necessárias para prevenção, detecção, resposta e recuperação;

14.194.3. Validar tecnicamente o funcionamento do ecossistema, com foco em cenários de ataque de segurança da informação;

14.194.4. Entregar à CONTRATANTE um ambiente monitorado, documentado e pronto para operação assistida.

14.195. Fases do Processo de set up e Implantação:

14.195.1. Planejamento e Kick-off:

14.195.1.1. Reunião de alinhamento inicial com as equipes da CONTRATANTE e CONTRATADA para definição de cronograma, papéis e responsabilidades;

14.195.1.2. Detalhar os objetivos e escopo da implantação da(s) solução(oes).

14.195.2. Setup e Configuração de Ambientes:

14.195.2.1. Preparação e validação de ambientes (on-premises e/ou nuvem), incluindo rede, conectividade segura, contas de serviço e mecanismos de autenticação;

14.195.2.2. Instalação, provisionamento e configuração inicial das soluções;

14.195.2.3. Implementação de controles de segurança na infraestrutura (segmentação, criptografia, hardening básico).

14.196. Conclusão dos Serviços de Setup e Implantação:

14.196.1. Após a conclusão dos serviços de setup e implantação, a(s) soluçao(oes) deverá(o) estar completamente disponível(eis) e funcional(ais), atendendo integralmente a todas as definições técnicas, funcionais e de segurança especificadas neste Termo de Referência. A homologação da(s) soluçao(oes), por parte da CONTRATANTE, será(o) realizada(s) com base na comprovação de que a(s) solução(oes) está(o) em pleno funcionamento, com todas as integrações configuradas os módulos operacionais e conforme as condições estabelecidas neste Termo de Referência;

14.196.2. A prestação dos serviços de operação assistida deverá ser objeto de validação e aprovação mensal formal por parte da CONTRATANTE, condição indispensável para a liberação dos pagamentos devidos à CONTRATADA relativos ao período de competência;

14.196.3. Para tanto, ao final de cada mês, a CONTRATADA deverá apresentar relatório técnico detalhado dos serviços prestados, contendo, no mínimo: atividades realizadas, horas ou capacidade empregada, incidentes tratados, indicadores de desempenho (KPIs e SLAs), treinamentos executados, entregáveis produzidos e eventuais não conformidades identificadas, bem como o plano de ação correspondente. Este relatório será analisado pelos responsáveis designados pela CONTRATANTE, que poderão solicitar esclarecimentos, complementações ou ajustes antes da emissão do aceite;

14.196.4. A validação mensal, formalizada por meio de documento de aceite (físico ou eletrônico) emitido pela CONTRATANTE, é fundamental para:

14.196.4.1. Assegurar a transparência na execução contratual, permitindo a rastreabilidade entre serviços executados e valores faturados;

14.196.4.2. Garantir a eficiência e aderência dos serviços às diretrizes técnicas, operacionais e de negócio do projeto governamental;

14.196.4.3. Viabilizar o acompanhamento tempestivo de desvios de escopo, qualidade ou desempenho, possibilitando sua correção antes que se tornem recorrentes;

14.196.4.4. Comprovar, perante órgãos de controle interno e externo, a regularidade da execução e a compatibilidade entre o objeto contratado e os recursos públicos despendidos;

14.196.4.5. Fica estabelecido que a emissão de faturas pela CONTRATADA deverá estar vinculada à apresentação do relatório mensal e à obtenção do respectivo aceite pela CONTRATANTE. Na hipótese de não validação dos

serviços, seja por ausência de entrega do relatório, por descumprimento de obrigações contratuais, por não atingimento de níveis mínimos de serviço (SLAs) ou por outras não conformidades relevantes, a CONTRATANTE poderá:

14.196.4.5.1. reter, glosar ou suspender o pagamento total ou parcial relativo ao período;

14.196.4.5.2. exigir a correção das falhas sem ônus adicional;

14.196.4.5.3. aplicar as sanções administrativas cabíveis, nos termos da legislação vigente e do contrato (advertência, multa, suspensão de contratar, entre outras).

14.196.5. Esse processo de validação deverá ser conduzido de forma formal e documentada, observando:

14.196.5.1. Registro de todos os relatórios, pareceres, comunicações e termos de aceite em sistema oficial da CONTRATANTE;

14.196.5.2. Participação dos responsáveis técnicos e gestores do contrato;

14.196.5.3. Prazos definidos para análise, manifestação e eventual contestação.

Serviço de Operação Assistida e treinamento para Plataforma unificada de segurança cibernética para proteção integrada de endpoints, proteção de e-mail, nuvem, identidade, rede, dados, campanha de pishing, EDR, DLP e usuários com automação inteligente

14.197. Objeto do Serviço de Operação Assistida:

14.197.1. O serviço de operação assistida tem como objeto apoiar a CONTRATANTE na operação contínua da plataforma unificada de segurança cibernética para proteção integrada de endpoints, e-mail, nuvem, identidade, rede, dados, campanhas de phishing, EDR, DLP e usuários, com automação inteligente, garantindo seu uso adequado, eficaz e alinhado às melhores práticas e normas aplicáveis.

14.198. Objetivos Específicos:

14.198.1. Assegurar a operação estável, segura e contínua de todos os módulos da plataforma unificada (endpoint, e-mail, nuvem, identidade, rede, dados, EDR, DLP, campanhas de phishing e awareness);

14.198.2. Garantir que as funcionalidades de detecção, prevenção e resposta automática sejam corretamente configuradas, ajustadas e acompanhadas, maximizando a eficácia da automação inteligente da solução (por exemplo, auto-remediação, correlação de eventos);

14.198.3. Reduzir o tempo de detecção e resposta a incidentes de segurança, com priorização baseada em risco e impacto para o negócio da CONTRATANTE;

14.198.4. Apoiar a equipe interna da CONTRATANTE em atividades de 2º e 3º nível, fornecendo orientação técnica especializada e executando, quando previsto, ações diretamente na plataforma;

14.198.5. Promover transferência de conhecimento estruturada, para aumentar a autonomia da CONTRATANTE na operação diária da plataforma;

14.198.6. Prover evidências de conformidade com a LGPD e demais normativos de segurança da informação aplicáveis ao órgão, por meio de relatórios, registros de incidentes e trilhas de auditoria.

14.199. Escopo e Requisitos do Serviço:

14.199.1. Apoio à resposta a incidentes:

14.199.1.1. Apoiar a CONTRATANTE na execução de ações como: isolamento de endpoints, bloqueio de contas ou sessões, ajuste/bloqueio de regras de DLP, bloqueio de domínios/IPs, revogação de tokens, quarentena de e-mails e arquivos, entre outras;

14.199.1.2. Participar de análises pós-incidente (post-mortem), produzindo relatório com causa raiz, impacto e recomendações de melhoria.

14.199.2. Gestão de políticas e ajustes finos:

14.199.2.1. Apoiar a definição, criação e revisão de políticas de EDR, antivírus/NGAV, DLP, proteção de e-mail, controle de acesso à nuvem, identidade e rede;

14.199.2.2. Realizar ajustes de regras, listas de bloqueio/permissão, níveis de sensibilidade e automações, visando reduzir falsos positivos e aumentar a eficácia da detecção.

14.199.3. Campanhas de phishing e awareness:

14.199.3.1. Apoiar o planejamento, configuração, execução e análise de campanhas de phishing simuladas;

14.199.3.2. Produzir relatórios de desempenho dos usuários, recomendar trilhas de treinamento e apoiar na integração com o módulo de conscientização da plataforma.

14.199.4. Relatórios e painéis executivos:

14.199.4.1. Elaborar relatórios periódicos (mínimo mensal) com: panorama de ameaças, incidentes tratados, recomendações de melhoria, aderência a políticas, indicadores de risco e de conformidade;

14.199.4.2. Apoiar a construção de dashboards específicos para a alta gestão e para áreas técnicas.

14.199.5. Transferência de conhecimento e documentação:

14.199.5.1. Produzir e manter atualizados manuais operacionais, procedimentos (runbooks), FAQs e guias de uso da plataforma;

14.199.5.2. Realizar treinamentos para à equipe da CONTRATANTE, com registro de presença e material didático, esse treinamento poderá ser ministrado virtualmente.

14.200. Requisitos de equipe do prestador:

14.200.1. Disponibilizar equipe multidisciplinar com, no mínimo:

14.200.1.1. 01 Responsável Técnico;

14.200.1.2. 01 (um) analista de segurança pleno/júnior para sustentação operacional.

14.201. Requisitos de governança:

14.201.1. Realização de reunião operacional periódica (Quinzenal) para revisar incidentes, problemas recorrentes e alterações relevantes;

14.201.2. Realização de reunião executiva mensal para apresentar relatório consolidado de riscos, incidentes, melhorias e revisar KPIs e plano de ação.

Serviço de Operação Assistida e Treinamento para Solução de Detecção e Resposta a Incidentes em Endpoints (EDR)

14.202. Objeto do Serviço de Operação Assistida em EDR:

14.202.1. O serviço de operação assistida tem por objeto apoiar a CONTRATANTE na operação contínua da Solução de Detecção e Resposta a Incidentes em Endpoints (EDR), garantindo seu uso adequado, eficaz e alinhado às melhores práticas de segurança cibernética e às normas aplicáveis ao setor público;

14.202.2. O serviço abrangerá todos os endpoints contemplados no escopo do contrato (estações de trabalho, notebooks, servidores, dispositivos móveis quando suportados), em todos os ambientes da CONTRATANTE.

14.203. Objetivos Específicos:

14.203.1. Assegurar a operação estável, segura e contínua da solução de EDR, incluindo monitoramento, detecção, investigação e resposta a incidentes em endpoints;

14.203.2. Garantir que as funcionalidades de análise comportamental, detecção avançada, automação de resposta e correlação de eventos do EDR sejam corretamente configuradas e mantidas;

14.203.3. Reduzir o tempo de detecção e resposta (MTTD/MTTR) a incidentes de segurança em endpoints, priorizando aqueles com maior impacto potencial para a CONTRATANTE;

14.203.4. Apoiar a equipe interna da CONTRATANTE em atividades de 2º e 3º nível relacionadas ao EDR, incluindo análise de alertas, investigação de incidentes e recomendação de medidas corretivas;

14.203.5. Promover transferência de conhecimento estruturada sobre a operação do EDR, aumentando a autonomia da CONTRATANTE ao longo da vigência contratual;

14.203.6. Prover evidências de conformidade (logs, relatórios, trilhas de auditoria) para atender a LGPD, políticas internas de segurança da informação e exigências de órgãos de controle.

14.204. Escopo e Requisitos do Serviço de Operação Assistida em EDR:

14.204.1. Análise e investigação de incidentes em endpoints;

14.204.2. Analisar cadeias de ataque (kill chain), árvores de processos, conexões de rede e indicadores de comprometimento (IOCs) detectados pelo EDR;

14.204.3. Reconstruir a linha do tempo do incidente (timeline), identificando vetor de entrada, movimentação lateral e impacto;

14.204.4. Recomendação e/ou execução de medidas de resposta;

14.204.5. Orientar e, quando previsto no contrato, executar ações de resposta, tais como:

14.204.5.1. Isolamento de endpoints da rede (mantendo canal de gestão);

14.204.5.2. Bloqueio/encerramento de processos maliciosos;

14.204.5.3. Exclusão/quarentena de arquivos;

14.204.5.4. Remoção de persistência e correção de configurações;

14.204.5.5. Aplicação de bloqueios adicionais (hash, caminho, editor, assinatura).

14.205. Gestão de políticas e ajustes finos do EDR:

14.205.1. Apoiar a criação, revisão e manutenção de políticas de detecção e resposta, incluindo:

14.205.1.1. Regras comportamentais;

14.205.1.2. Listas de permissão/bloqueio (allowlist/denylist);

14.205.1.3. Exceções justificadas para aplicações legítimas (false positives);

14.205.1.4. Ajustar níveis de sensibilidade e regras para reduzir falsos positivos e falsos negativos;

14.205.1.5. Integração com outros sistemas.

14.205.2. Apoiar a integração do EDR com sistemas de SIEM, SOAR e ITSM da CONTRATANTE, quando existentes, garantindo:

14.205.2.1. Exportação de logs em formatos padrão (JSON, syslog, CEF);

14.205.2.2. Geração automática de tickets de incidente;

14.205.2.3. Correlação de eventos de endpoint com outros vetores (rede, identidade, e-mail etc.), quando aplicável.

14.206. Relatórios e painéis:

14.206.1. Elaborar relatórios periódicos (mensais) contendo:

14.206.1.1. Resumo dos incidentes tratados;

14.206.1.2. Tipos de ameaças identificadas (ransomware, trojans, living-off-the-land, etc.);

14.206.1.3. Tendências por unidade, grupo de usuários e tipo de endpoint;

14.206.1.4. Recomendações de hardening e melhorias;

14.206.1.5. Apoiar a construção de painéis no console do EDR para diferentes perfis (técnico, gestor, executivo);

14.206.1.6. Transferência de conhecimento e documentação;

14.206.1.7. Elaborar e manter atualizados;

14.206.1.8. Procedimentos operacionais padrão (POPs/runbooks) para incidentes típicos;

14.206.1.9. Guias de uso da console de EDR;

14.206.1.10. Boas práticas de resposta em endpoints.

14.206.2. Realizar treinamento para a equipe da CONTRATANTE, com foco em:

14.206.2.1. Interpretação de alertas;

14.206.2.2. Execução de ações básicas no EDR;

14.206.2.3. Fluxos de escalonamento interno;

14.206.2.4. Requisitos de equipe do prestador;

14.206.2.5. Disponibilizar equipe com, no mínimo:

14.206.2.5.1. 01 (um) Responsavel técnico / especialista em EDR;

14.206.2.5.2. 01 (um) analista pleno/júnior para sustentação operacional do EDR.

14.206.2.6. Realização de reuniões operacionais periódicas (quinzenal) para:

14.206.2.6.1. Revisar incidentes recentes;

14.206.2.6.2. Avaliar regras e políticas de detecção;

14.206.2.6.3. Identificar incidentes recorrentes e oportunidades de melhoria.

14.206.2.7. Realização de reuniões executivas mensais para:

14.206.2.7.1. Apresentar relatório consolidado de incidentes, riscos e tendências;

14.206.2.7.2. Propor melhorias de hardening, segmentação e políticas;

14.206.2.7.3. Revisar KPIs e acordar planos de ação;

14.206.2.7.4. Definir fluxos de comunicação e escalonamento com pontos focais da CONTRATANTE (técnicos e de gestão).

Serviço de Operação Assistida e Treinamento para Solução de Proteção e Prevenção de Vazamento de Dados (DLP)

14.207. Objeto do Serviço de Operação Assistida em DLP:

14.207.1. O serviço de operação assistida tem por objeto apoiar a CONTRATANTE na operação contínua da Solução de Proteção e Prevenção de Vazamento de Dados (DLP), abrangendo dados em uso, em trânsito e em repouso, em endpoints, e-mail, aplicações em nuvem e demais vetores contemplados no contrato;

14.207.2. O serviço visa garantir que a solução de DLP seja configurada, monitorada e evoluída de forma alinhada às melhores práticas de mercado, às necessidades de negócio da CONTRATANTE e às exigências regulatórias aplicáveis (especialmente LGPD e normas internas de segurança da informação).

14.208. Objetivos Específicos:

14.208.1. Assegurar a operação estável e eficaz da solução de DLP, com políticas adequadas para proteção de dados pessoais, dados sensíveis, informações sigilosas e demais dados críticos da CONTRATANTE;

14.208.2. Implementar e manter políticas de DLP contextuais e baseadas em risco, minimizando vazamentos acidentais ou maliciosos em múltiplos vetores (USB, e-mail, nuvem, impressão, compartilhamentos, etc.);

14.208.3. Reduzir o número e o impacto de incidentes de vazamento de dados, melhorando o tempo de detecção, resposta e remediação;

14.208.4. Apoiar a equipe interna da CONTRATANTE na análise de incidentes de DLP, definição de exceções justificadas e ajustes finos de políticas para reduzir falsos positivos e evitar bloqueios indevidos;

14.208.5. Promover transferência de conhecimento estruturada sobre o uso e a operação da solução de DLP, aumentando a autonomia da CONTRATANTE;

14.208.6. Prover evidências e relatórios de conformidade que suportem auditorias internas/externas e demonstração de aderência à LGPD e demais normativos de segurança da informação;

14.209. Escopo e Requisitos do Serviço de Operação Assistida em DLP:

14.209.1. Mapeamento e classificação de dados:

14.209.1.1. Apoiar a CONTRATANTE no mapeamento de categorias de dados a serem protegidos (por exemplo: PII, dados sensíveis, dados financeiros, informações estratégicas, segredos de negócio);

14.209.1.2. Auxiliar na configuração e manutenção de mecanismos de classificação automática e baseada em conteúdo/contexto (padrões pré-definidos, expressões regulares, dicionários, rótulos de classificação, etc).

14.209.2. Configuração e gestão de políticas de DLP:

14.209.2.1. Definir, em conjunto com a CONTRATANTE, políticas de DLP por tipo de dado, vetor (endpoint, e-mail, nuvem, web, USB) e perfil de usuário/área;

14.209.2.2. Configurar ações de resposta (bloquear, permitir com alerta, criptografar, registrar somente, solicitar justificativa) em função da criticidade do dado e do contexto de uso;

14.209.2.3. Criar e gerenciar exceções controladas, com base em aprovação formal e prazo de validade.

14.210. Resposta a incidentes de vazamento de dados

14.210.1. Apoiar a CONTRATANTE em ações como:

14.210.1.1. Bloqueio imediato de fluxos não autorizados (e-mail, uploads, compartilhamentos);

14.210.1.2. Revogação de acessos ou compartilhamentos indevidos em nuvem;

14.210.1.3. Criptografia ou quarentena de arquivos em endpoints;

14.210.1.4. Execução de varreduras retroativas para identificar outras ocorrências semelhantes.

14.210.2. Apoiar na elaboração de relatórios de incidentes que possam ser utilizados em comunicações formais:

14.210.2.1. Integração com outros módulos e sistemas.

14.210.3. Apoiar a integração da solução de DLP com:

14.210.3.1. Módulos de e-mail, nuvem e endpoint já contratados;

14.210.3.2. Sistemas de SIEM/SOAR para correlação de eventos;

14.210.3.3. Sistemas de ITSM/Service Desk para abertura e acompanhamento automático de tickets de DLP.

14.210.4. Relatórios e dashboards de governança de dados:

14.210.4.1. Elaborar relatórios periódicos (mensal) com:

14.210.4.1.1. Incidentes de DLP por tipo de dado, unidade, usuário e vetor;

14.210.4.1.2. Tendências de risco (ex.: aumento de tentativas de exfiltração via e-mail ou nuvem);

14.210.4.1.3. Principais causas e recomendações de mitigação.

14.210.5. Apoiar na criação de painéis específicos para:

14.210.5.1. Gestores de segurança da informação;

14.210.5.2. Gestores de áreas de negócio;

14.210.5.3. Alta administração (visão executiva consolidada).

14.210.6. Transferência de conhecimento e documentação:

14.210.6.1. Desenvolver e manter atualizados:

14.210.6.1.1. Procedimentos operacionais padrão (POPs/runbooks) para tratamento de incidentes de DLP;

14.210.6.1.2. Guias de configuração e operação da solução;

14.210.6.1.3. Catálogo de políticas de DLP vigentes (com descrição, escopo e responsáveis).

14.210.6.2. Realizar treinamento voltado à equipe de segurança, TI e, quando aplicável, aos “data owners” e “data stewards” designados pela CONTRATANTE.

14.211. Requisitos de equipe do prestador:

14.211.1. Disponibilizar equipe com, no mínimo:

14.211.1.1. 01 (um) Responsavel Técnico;

14.211.1.2. 01 (um) analista pleno/júnior para suporte operacional de DLP.

14.212. Requisitos de governança:

14.212.1. Realização de reuniões operacionais periódicas (quinzenal) para:

14.212.1.1. Revisar incidentes recentes;

14.212.1.2. Avaliar eficácia das políticas vigentes;

14.212.1.3. Ajustar regras, exceções e fluxos.

14.212.2. Realização de reuniões executivas mensais para:

14.212.2.1. Apresentar panorama de risco de vazamento de dados;

14.212.2.2. Discutir recomendações de melhoria e priorização de ações (técnicas e organizacionais);

14.212.2.3. Estabelecer fluxo de comunicação com os responsáveis internos por privacidade e proteção de dados.

Serviço de Operaçao Assistida e Treinamento para Plataforma de Avaliação de Maturidade de Segurança da Informação com foco específico na capacidade de prevenção, detecção, resposta e recuperação

14.213. Avaliar as políticas existentes de governança, identidade, proteção, detecção, resposta e recuperação;

14.214. Validar a aderência dessas políticas aos frameworks como NIST CSF v2 & AI RMF (Artificial Intelligence Risk Management Framework), NIST SP 800-30 - Avaliação de Risco (Risk Assessments), NIST SP 800-12 - Introdução à Segurança da Informação, NIST SP 800-39 - Gestão de Riscos Organizacionais, NIST SP 800-88 - Sanitização de Mídias, CIS Controls v8 Center for Internet Security, ISO 27001 - Information Security, Cybersecurity and Privacy protection, Cyber Insurance, ISO 27701 - Privacy Information Management, ISO 27005 - Information Security Risk Management, ISO 22301 - Business continuity management systems, ISO 23894 - Artificial intelligence — Guidance on risk management, entre outros;

14.215. Sugerir atualizações ou ajustes com base em melhores práticas e requisitos regulatórios;

14.216. Relatórios de Maturidade:

14.216.1. Geração de Relatório Consolidado de Maturidade Cibernética, que fornecerá a visão unificada da postura de segurança do órgão com base em três frameworks de referência: NIST, CIS Controls, ISO 27001 e LGPD;

14.216.2. Relatório de Maturidade NIST Cybersecurity Framework (CSF):

14.216.2.1. Apresentação do Nível de Maturidade Atual do órgão (e.g., Nível 2 - Risco Repetível para Nível 3 - Risco Adaptativo);

14.216.2.2. O relatório deve detalhar o Atingimento Percentual em cada uma das cinco funções do NIST: Identificar, Proteger, Detectar, Responder e Recuperar, destacando os gaps estratégicos e o progresso do roadmap de melhoria;

14.216.2.3. Relatório de Aderência aos CIS Controls (Centro de Segurança da Internet);

14.216.2.4. Demonstração do score de aderência e da eficácia dos controles de segurança mais críticos. O relatório deve priorizar a remediação com base na capacidade dos controles de deter as táticas de ataque mais comuns. Ideal para o público técnico, mostrando a eficiência na implementação da segurança básica.

14.216.3. Relatório de Conformidade ISO/IEC 27001 (Sistema de Gestão da Segurança da Informação – SGSI):

14.216.3.1. Avaliação formal da aderência aos requisitos da norma (Seção 4 a 10) e aos controles do anexo A (ISO 27002). O Consultor deve atestar a existência e a eficácia dos controles de Pessoas e Processos (e.g., Gestão de Acessos, Treinamento, Política de Continuidade), crucial para a demonstração de conformidade em auditorias externas.

14.216.4. Relatório de Status de Conformidade LGPD;

14.216.5. Traduzir os resultados complexos de segurança (NIST, CIS, ISO) em termos de negócio claros para o Comitê de Governança, facilitando a tomada de decisão sobre o aporte de capital e recursos humanos.

14.217. Geração e Validação de Controles de Auditoria:

14.217.1. Criar e revisar controles manuais e automatizados com base nos domínios e políticas da organização;

14.217.2. Garantir que os controles estejam alinhados com os requisitos de auditorias como PCI, ISO 27001, SOC2;

14.217.3. Pontuação de Conformidade e Planos de Ação;

14.217.4. Avaliar o nível de conformidade por tecnologia, processo e controle;

14.217.5. Medir o percentual de aplicação dos controles e sugerir:

14.217.5.1. Tecnologias adequadas;

14.217.5.2. Processos otimizados;

14.217.5.3. Serviços complementares.

14.218. Automação e Monitoramento Contínuo:

14.218.1. Configurar e manter os controles automatizados de conformidade;

14.218.2. Garantir que os dados estejam sempre atualizados para geração de relatórios em tempo real;

14.218.3. O serviço deverá ser executado através de atividades a serem desenvolvidas em reuniões, presenciais e/ou virtuais, devendo-se focar no detalhamento do plano de execução dos serviços, contemplando a metodologia de gestão, macro programa, plano de comunicação, relatórios de status e interfaces;

14.218.4. Nas reuniões de início deverão obrigatoriamente ser tratados os temas:

14.218.4.1. Aplicação da plataforma em seus aspectos direcionados à Administração Pública;

14.218.4.2. A importância da conformidade para a CONTRATANTE;

14.218.4.3. O projeto de adequação ao ambiente da CONTRATADA;

14.218.4.4. A definição e apresentação dos relatórios mensais;

14.218.4.5. As reuniões de planejamento entre CONTRATANTE e a CONTRATADA seguirão um cronograma a ser firmado em até 2 (dois) dias úteis após o início da prestação do serviço, dado o prazo exíguo da execução da fase, e poderão ser realizadas de forma remota, desde que acordado entre as partes.

14.219. Disponibilizar equipe mínima composta por:

14.219.1. 01 (um) Responsável Técnico Especialista;

14.219.2. 01 (um) Consultor Sênior especialista em segurança da informação.

14.220. Treinamento da Plataforma:

14.220.1. O treinamento devera focar nas capacidades de prevenção, detecção, resposta e recuperação, e tem por objetivo garantir que a CONTRATANTE utilize a solução de forma plena, consistente e alinhada às diretrizes do projeto governamental.

14.221. Objetivos Específicos do Treinamento:

14.221.1. O treinamento deverá capacitar os participantes para compreender os conceitos fundamentais de maturidade em segurança da informação, incluindo modelos de referência (por exemplo, NIST CSF, ISO 27001/27002, frameworks de maturidade) e sua aplicação em órgãos públicos;

14.221.2. Utilizar adequadamente a Plataforma de Avaliação de Maturidade para:

14.221.2.1. Realizar diagnósticos estruturados de maturidade de segurança da informação;

14.221.2.2. Mapear controles e capacidades nas dimensões de prevenção, detecção, resposta e recuperação;

14.221.2.3. Registrar evidências, planos de ação e responsáveis;

14.221.2.4. Interpretar relatórios, painéis e indicadores de maturidade, incluindo:

14.221.2.4.1. Níveis de maturidade por domínio de segurança;

14.221.2.4.2. Lacunas (gaps) entre a situação atual e o nível desejado;

14.221.2.4.3. Prioridades de evolução, considerando risco e criticidade institucional.

14.221.2.5. Planejar e acompanhar planos de melhoria contínua, utilizando a plataforma para:

14.221.2.5.1. Registrar ações, prazos, responsáveis e status;

14.221.2.5.2. Acompanhar a evolução da maturidade ao longo do tempo.

14.221.2.6. Apoiar a conformidade com normas e exigências de órgãos de controle, por meio da geração de evidências e relatórios estruturados extraídos da solução.

14.222. Público-alvo:

14.222.1. O treinamento destina-se, no mínimo, aos seguintes perfis:

14.222.1.1. Equipe de Segurança da Informação.

14.222.1.1.1. Gestores e analistas responsáveis pela elaboração e execução da Política de Segurança da Informação (PSI), gestão de riscos e planos de continuidade.

14.222.1.2. Gestores de TI e áreas correlatas:

14.222.1.2.1. Responsáveis pela infraestrutura, aplicações, redes e serviços de TI que alimentam ou são avaliados pela plataforma.

14.222.1.3. Gestores de Áreas de Negócio Críticas:

14.222.1.3.1. Representantes de áreas que detêm processos e dados sensíveis, responsáveis por validar informações e apoiar a priorização de ações.

14.222.1.4. Equipe de Governança, Riscos e Compliance (GRC):

14.222.1.4.1. Profissionais envolvidos em auditorias, riscos, conformidade com LGPD, normas internas e exigências de órgãos de controle;

14.222.1.4.2. Opcionalmente, outros stakeholders indicados pela CONTRATANTE, como membros de comitês de segurança ou de governança de TI.

Serviço de Operação Assistida e Treinamento para Solução de backup em nuvem e recuperação de desastres (DR) focada em proteção e rápida recuperação diante de ataques

14.223. Objeto do Serviço de Operação Assistida em Backup em Nuvem e DR:

14.223.1. O serviço de operação assistida tem por objeto apoiar a CONTRATANTE na operação contínua da Solução de backup em nuvem e recuperação de desastres (DR), focada em proteção e rápida recuperação diante de ataques, garantindo que os dados e sistemas críticos estejam protegidos, íntegros e recuperáveis dentro dos prazos e níveis de serviço exigidos;

14.223.2. O serviço abrangerá todos os ativos contemplados no escopo do contrato (servidores, bancos de dados, aplicações, endpoints, máquinas virtuais, dados em nuvem e, quando aplicável, ambientes SaaS), assegurando que as políticas de backup, replicação e

recuperação estejam alinhadas às melhores práticas de mercado e às necessidades de continuidade de negócio da CONTRATANTE.

14.224. Objetivos Específicos:

14.224.1. Assegurar a operação estável, segura e contínua da solução de backup em nuvem e DR, com monitoramento proativo de jobs, replicações e snapshots;

14.224.2. Garantir que as políticas de backup e retenção estejam configuradas de acordo com os requisitos de negócio, normativos e de segurança da CONTRATANTE, incluindo proteção contra ransomware (imutabilidade, air-gap lógico, etc.);

14.224.3. Reduzir o tempo de recuperação (RTO) e o ponto de recuperação (RPO) para cenários de desastre, ataques cibernéticos ou falhas operacionais, por meio de planos de DR testados e otimizados;

14.224.4. Apoiar a equipe interna da CONTRATANTE na gestão de incidentes de indisponibilidade ou perda de dados, incluindo a execução de procedimentos de restauração e failover;

14.224.5. Promover transferência de conhecimento estruturada sobre a operação da solução de backup e DR, aumentando a autonomia da CONTRATANTE;

14.224.6. Prover evidências de conformidade (relatórios de backup, logs de recuperação, testes de DR) para atender a LGPD, políticas internas e exigências de órgãos de controle.

14.225. Escopo e Requisitos do Serviço de Operação Assistida:

14.225.1. Configuração e gestão de políticas de backup e retenção:

14.225.1.1. Apoiar a CONTRATANTE na definição e configuração de políticas de backup adequadas a cada tipo de workload (servidores físicos, VMs, bancos de dados, endpoints, dados em nuvem, SaaS), considerando:

14.225.1.1.1. Frequência (diário, incremental, diferencial, contínuo) conforme definido entre a PROPONENTE e a CONTRATANTE;

14.225.1.1.2. Janelas de backup;

14.225.1.1.3. Períodos de retenção (curto, médio, longo prazo);

14.225.1.1.4. Políticas de imutabilidade e proteção contra exclusão/criptografia maliciosa.

14.225.1.2. Apoiar na configuraçao e manutençao das políticas de replicação para nuvem ou site de DR, garantindo que os dados estejam disponíveis em local geograficamente distinto;

14.225.1.3. Revisar periodicamente junto da equipe da CONTRATANTE as políticas para adequação a mudanças no ambiente, novos sistemas e requisitos regulatórios.

14.225.2. Proteção contra ransomware e ataques cibernéticos:

14.225.2.1. Garantir que a solução de backup esteja configurada com mecanismos de proteção anti-ransomware, incluindo:

14.225.2.1.1. Imutabilidade de backups (WORM – Write Once, Read Many);

14.225.2.1.2. Autenticação multifator (MFA) para operações críticas (exclusão de backups, alteração de políticas);

14.225.2.1.3. Isolamento lógico (air-gap) ou físico dos backups em relação à rede de produção;

14.225.2.1.4. Verificação de integridade dos backups antes da restauração.

14.225.2.2. Apoiar a CONTRATANTE na recuperação rápida em cenários de ataque, incluindo:

14.225.2.2.1. Restauração massiva de dados e sistemas;

14.225.2.2.2. Priorização de ativos críticos;

14.225.2.2.3. Utilização de snapshots ou réplicas para failover imediato.

14.225.3. Planos de recuperação de desastres (DR) e testes:

14.225.3.1. Apoiar a CONTRATANTE na elaboração e manutenção de planos de recuperação de desastres (DRP) baseados na solução contratada, contemplando:

14.225.3.1.1. Sequência de recuperação de sistemas e aplicações;

14.225.3.1.2. Procedimentos de failover e failback;

14.225.3.1.3. Pontos de contato e responsabilidades;

14.225.3.1.4. Estimativas de RTO e RPO por serviço.

14.225.3.2. Realizar testes periódicos de DR trimestrais, incluido:

14.225.3.2.1. Testes de restauração de arquivos e bancos de dados;

14.225.3.2.2. Testes de failover de máquinas virtuais ou servidores;

14.225.3.2.3. Simulações de cenários de ransomware.

14.225.3.3. Documentar os resultados dos testes, apontar falhas e propor ações corretivas e de melhoria.

14.225.4. Resposta a incidentes de perda de dados ou indisponibilidade:

14.225.4.1. Apoiar a CONTRATANTE na execução de restaurações emergenciais, seguindo os planos de DR e priorizando ativos críticos;

14.225.4.2. Orientar e, quando previsto, executar procedimentos de failover para ambiente de DR e posterior failback para o ambiente principal.

14.225.5. Relatórios e dashboards:

14.225.5.1. Produzir relatórios periódicos (mensal) com:

14.225.5.1.1. Status de proteção por ativo e workload;

14.225.5.1.2. Taxa de sucesso de backups e replicações;

14.225.5.1.3. Incidentes de falha e ações corretivas;

14.225.5.1.4. Resultados de testes de DR;

14.225.5.1.5. Recomendações de melhoria.

14.225.6. Transferência de conhecimento e documentação:

14.225.6.1. Elaborar e manter atualizados:

14.225.6.1.1. Procedimentos operacionais padrão (POPs/runbooks) para restauração de diferentes tipos de workload;

14.225.6.1.2. Planos de recuperação de desastres (DRP);

14.225.6.1.3. Guias de uso da console de backup e DR;

14.225.6.1.4. Matriz de responsabilidades (RACI) entre fornecedor e CONTRATANTE.

14.225.6.2. Realizar treinamento para a equipe da CONTRATANTE sobre:

14.225.6.2.1. Operação da console de backup;

14.225.6.2.2. Execução de restaurações e failover;

14.225.6.2.3. Interpretação de relatórios e alertas;

14.225.6.2.4. Boas práticas de proteção de dados e continuidade.

14.225.7. Disponibilizar equipe mínima composta por:

14.225.7.1. 01 (um) Responsavel Tecnico Especialista em backup, recuperação de desastres e continuidade de negócios;

14.225.7.2. 01 (um) Analista pleno/júnior para suporte operacional.

14.225.8. Realizar:

14.225.8.1. Reuniões operacionais (quinzenais), a ser definido entre as partes no início do projeto, para revisar jobs de backup, falhas, capacidade e ajustes;

14.225.8.2. Reuniões executivas mensais para apresentação de resultados, riscos, testes de DR (quando for o prazo de testes de DR) e plano de melhoria.

Serviço de Operação Assistida e treinamento para Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM)

14.226. Objeto do Serviço de Operação Assistida em RMM:

14.226.1. Serviço de operação assistida tem por objeto apoiar a CONTRATANTE na operação contínua da Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM), abrangendo estações de trabalho, notebooks, servidores, dispositivos móveis (quando suportados) e demais ativos de TI previstos no contrato;

14.226.2. O serviço visa garantir que o RMM seja utilizado para monitorar, administrar, atualizar, gestão de vulnerabilidade e remediar remotamente os ativos de TI, de forma

padronizada, segura e alinhada às necessidades de negócio, requisitos técnicos e normativos da CONTRATANTE.

14.227. Objetivos Específicos:

14.227.1. Assegurar a operação estável e eficaz da solução de RMM como ferramenta central de gestão remota dos ativos de TI;

14.227.2. Implementar e manter rotinas de monitoramento, manutenção preventiva e corretiva, reduzindo indisponibilidades, falhas recorrentes e intervenções manuais on-site;

14.227.3. Reduzir o tempo de detecção e resolução de problemas em endpoints e servidores (MTTD/MTTR), através de alertas, automações e ações remotas padronizadas;

14.227.4. Apoiar a equipe interna da CONTRATANTE na gestão do parque de TI, incluindo inventário, aplicação de scripts, atualizações, políticas de configuração, gestao de vulnerabilidade e suporte remoto aos usuários;

14.227.5. Promover transferência de conhecimento estruturada sobre a operação do RMM, aumentando a autonomia da CONTRATANTE ao longo da vigência contratual;

14.227.6. Prover evidências de conformidade e rastreabilidade das ações realizadas nos ativos gerenciados, em atendimento a normas internas e órgãos de controle.

14.228. Escopo e Requisitos do Serviço de Operação Assistida em RM:

14.228.1. Realizar monitoramento (8x5 – horário comercial) dos ativos de TI cobertos pelo RMM, incluindo:

14.228.1.1. Disponibilidade de dispositivos;

14.228.1.2. Utilização de CPU, memória, disco e rede;

14.228.1.3. Status de serviços e processos críticos;

14.228.1.4. Alertas de falhas de hardware, espaço em disco, conectividade e outros parâmetros configurados.

14.228.2. Configurar e operar alertas automáticos para eventos relevantes (por exemplo: queda de servidor, falta de espaço em disco, serviços parados, falhas recorrentes);

14.228.3. Manter painéis de visibilidade em tempo quase real do estado de saúde do parque de TI, por unidade, tipo de ativo e criticidade.

14.229. Gestão remota e automações:

14.229.1. Apoiar a CONTRATANTE na definição e execução de tarefas de manutenção preventiva via RMM, tais como:

14.229.1.1. Limpeza de arquivos temporários;

14.229.1.2. Verificações de integridade de disco;

14.229.1.3. Reinicialização programada de serviços/sistemas;

14.229.1.4. Aplicação de ajustes de configuração padronizados.

14.229.2. Configurar e manter scripts e automações para tratamento de incidentes recorrentes, reduzindo a intervenção manual (por exemplo, restart de serviços, correção de chaves de registro, aplicação de correções simples);

14.229.3. Apoiar na distribuição remota de software e atualizações (quando previsto na solução de RMM ou integrado ao UEM/patching), garantindo padronização da base instalada.

14.230. Gestão de Vulnerabilidades:

14.230.1. O serviço deverá ser utilizar a plataforma de apoio à gestão de vulnerabilidades, permitindo identificar, priorizar e tratar vulnerabilidades em sistemas operacionais, softwares instalados e configurações de endpoints e servidores;

14.230.2. O prestador deverá apoiar a CONTRATANTE na coleta e consolidação de informações de inventário (versões de SO, aplicações, componentes, drivers, agentes) a partir do RMM, de forma a subsidiar:

14.230.2.1. A correlação com bases de vulnerabilidades (CVEs, boletins de segurança dos fabricantes, normativos internos);

14.230.2.2. A identificação de ativos mais expostos (por criticidade, obsolescência ou ausência de atualizações).

14.230.3. Deverão ser definidas, em conjunto com a CONTRATANTE, rotinas periódicas de varredura e análise de conformidade utilizando o RMM, incluindo:

14.230.3.1. Verificação de versões mínimas de SO e aplicações;

14.230.3.2. Identificação de softwares sem suporte ou não autorizados;

14.230.3.3. Checagem de parâmetros de segurança (por exemplo, firewall habilitado, serviços desnecessários, configurações de criptografia, etc.).

14.230.4. O prestador deverá utilizar as capacidades de automação e scripting do RMM para apoiar o tratamento de vulnerabilidades, sempre que possível, incluindo:

14.230.4.1. Aplicação de correções ou ajustes de configuração padronizados;

14.230.4.2. Desinstalação remota de softwares obsoletos ou proibidos;

14.230.4.3. Execução de scripts de hardening alinhados às boas práticas da CONTRATANTE.

14.230.5. Os resultados das ações de gestão de vulnerabilidades realizadas via RMM deverão ser documentados e reportados mensalmente, contemplando:

14.230.5.1. Quantidade e tipos de vulnerabilidades identificadas por classe de ativo;

14.230.5.2. Ações de mitigação executadas (correções aplicadas, softwares removidos, ajustes de configuração);

14.230.5.3. Itens pendentes com justificativa (por exemplo, dependência de sistema legado, janelas de manutenção);

14.230.5.4. Recomendações de priorização para tratamento manual ou com outras ferramentas especializadas (como scanners de vulnerabilidade dedicados, quando existentes).

14.230.6. A atuação do RMM na gestão de vulnerabilidades deverá ser alinhada aos processos formais de gestão de vulnerabilidades da CONTRATANTE (caso existentes) e às boas práticas de frameworks como NIST CSF e ISO 27002, servindo como camada operacional de execução (discovery, correção e verificação) das ações aprovadas;

14.230.7. O prestador deverá garantir que ações de correção de vulnerabilidades via RMM sejam planejadas e controladas, observando:

14.230.7.1. Janelas de mudança acordadas;

14.230.7.2. Testes prévios em ambiente piloto quando necessário.

14.230.8. Suporte remoto aos usuários e ativos:

14.230.8.1. Apoiar a operação do módulo de acesso remoto do RMM, permitindo que a equipe de TI da CONTRATANTE preste suporte a usuários de forma segura e rastreável, incluindo:

14.230.8.1.1. Controle remoto de telas;

14.230.8.1.2. Execução de comandos remotos;

14.230.8.1.3. Transferência de arquivos quando necessário e permitido.

14.230.8.2. Auxiliar na definição de políticas de autorização e privacidade para sessões de suporte remoto (por exemplo, necessidade de consentimento do usuário final, avisos na tela, logs de sessão).

14.230.9. Inventário e padronização de ativos:

14.230.9.1. Apoiar a CONTRATANTE na configuração e uso do inventário automático de hardware e software do RMM, garantindo:

14.230.9.1.1. Visão consolidada do parque de TI (equipamentos, modelos, sistemas operacionais, softwares instalados);

14.230.9.1.2. Identificação de ativos obsoletos, fora de suporte ou não conformes com o padrão definido;

14.230.9.1.3. Auxiliar na padronização de configurações por grupos de dispositivos (por exemplo, políticas por unidade, por função ou criticidade).

14.230.10. Integração com outras ferramentas:

14.230.10.1. Apoiar a integração do RMM com:

14.230.10.1.1. Sistemas de ITSM/Service Desk (abertura/atualização automática de tickets a partir de alertas, caso exista);

14.230.10.1.2. Eventuais soluções de SIEM para envio de logs de ações administrativas;

14.230.10.1.3. Outras soluções de gestão (por exemplo, UEM, patch management, antivírus/EDR), quando aplicável.

14.230.11. Relatórios e dashboards de operação de TI:

14.230.11.1. Produzir relatórios Mensal com:

14.230.11.1.1. Disponibilidade e saúde dos ativos;

14.230.11.1.2. Incidentes recorrentes e ações remotas executadas;

14.230.11.1.3. Tempo médio de resposta e resolução;

14.230.11.1.4. Aderência a padrões de configuração;

14.230.11.1.5. Evolução do parque (novos ativos, descomissionamentos, obsolescência).

14.230.11.2. Apoiar a construção de dashboards no RMM ou ferramentas correlatas, para:

14.230.11.2.1. Equipes técnicas (visão detalhada de alertas, automações, scripts);

14.230.11.2.2. Gestão de TI (indicadores de produtividade, estabilidade e conformidade);

14.230.11.2.3. Alta administração (visão executiva da saúde geral da infraestrutura).

14.230.12. Transferência de conhecimento:

14.230.12.1. Elaborar e manter atualizados:

14.230.12.1.1. Procedimentos operacionais padrão (POPs/runbooks) para uso do RMM em atividades comuns (onboarding de ativos, aplicação de scripts, suporte remoto, resolução de alertas frequentes);

14.230.12.1.2. Catálogo de automações e scripts utilizados;

14.230.12.1.3. Matriz de responsabilidades (RACI) entre fornecedor e CONTRATANTE na operação do RMM.

14.230.12.2. Realizar treinamento para a equipe da CONTRATANTE sobre:

14.230.12.2.1. Uso da console do RMM;

14.230.12.2.2. Interpretação de alertas e dashboards;

14.230.12.2.3. Execução de scripts e tarefas remotas;

14.230.12.2.4. Boas práticas de suporte remoto e gestão de ativos;

14.230.12.2.5. Requisitos de Equipe do Prestador.

14.230.13. Disponibilizar equipe mínima composta por:

14.230.13.1. 01 (um) Especialista em gestão remota de ativos / RMM (líder técnico);

14.230.13.2. 01 (um) Analista pleno/júnior para suporte operacional e monitoramento diário.

14.230.14. Realizar:

14.230.14.1. Reuniões operacionais (quinzenais) para revisão de alertas, automações, scripts e incidentes recorrentes;

14.230.14.2. Reuniões executivas mensais para apresentação de indicadores de desempenho da operação remota, riscos e plano de melhoria.

Serviço de Operação Assistida e treinamento para Solução de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados

14.231. Objetivo do serviço de Operação Assistida e Suporte Técnico Especializado:

14.231.1. O serviço de operação assistida e suporte técnico especializado tem por objetivo manter em pleno funcionamento operacional a solução fornecida, assegurando sua disponibilidade, atualização, correção de falhas e evolução contínua, em alinhamento às melhores práticas do fabricante, aos requisitos técnicos e às diretrizes da CONTRATANTE.

14.232. Manutenção Operacional e Suporte Técnico:

14.232.1. A CONTRATADA deverá prestar suporte técnico contínuo para a desinstalação, reconfiguração ou reinstalação de componentes da solução, sempre que tais ações forem decorrentes de:

14.232.1.1. falhas de software;

14.232.1.2. atualizações de versão;

14.232.1.3. correção de defeitos;

14.232.1.4. ajustes e reparos necessários.

14.232.2. Tais atividades deverão ser executadas em conformidade com:

14.232.2.1. os manuais oficiais da solução;

14.232.2.2. as normas técnicas específicas aplicáveis;

14.232.2.3. melhores práticas recomendadas pelo fabricante.

14.232.3. A CONTRATADA deverá prestar suporte na revisão, manutenção e melhorias da solução, incluindo:

14.232.3.1. ajustes de parâmetros e políticas;

14.232.3.2. otimização de desempenho;

14.232.3.3. adequações decorrentes de novas recomendações do fabricante ou de lições aprendidas em produção.

14.233. Atualização de Conteúdo de Segurança:

14.233.1. A CONTRATADA deverá manter índice de atualização do conteúdo de segurança (por exemplo, agentes, sensores, assinaturas, motores de detecção, módulos de proteção) acima de 90% em relação ao parque instalado, observadas as limitações de compatibilidade com o sistema operacional de cada endpoint;

14.233.2. Entende-se por índice de atualização acima de 90% a condição em que mais de 90% das máquinas gerenciadas estão, em caráter contínuo, com as últimas atualizações disponíveis do fabricante, dentro das políticas aprovadas pela CONTRATANTE;

14.233.3. O indicador de atualização deverá ser:

14.233.3.1. extraído diretamente da plataforma de administração/gerência da solução;

14.233.3.2. apresentado em relatórios periódicos de operação assistida;

14.233.3.3. utilizado como métrica para acompanhamento de desempenho e governança.

14.234. Planejamento de Ações Preventivas e Corretivas:

14.234.1. Sempre que forem necessárias ações preventivas ou corretivas com potencial impacto em produção (por exemplo, atualizações de versão, mudanças de configuração ampla, reconfiguração de políticas, reinstalação em larga escala), a CONTRATADA deverá:

14.234.1.1. Agendar previamente as intervenções junto à CONTRATANTE;

14.234.1.2. Observar os horários e janelas de manutenção definidos pela CONTRATANTE;

14.234.1.3. Apresentar, quando solicitado, plano de mudança contendo escopo, riscos, plano de rollback e responsáveis.

14.234.2. A execução dessas ações deverá respeitar os processos de gestão de mudanças da CONTRATANTE, quando existentes (por exemplo, ITIL/ITSM).

14.235. Atividades Abrangidas pelo Serviço de Operação Assistida

14.235.1. Como parte do serviço de operação assistida e suporte técnico especializado prestado pela CONTRATADA, deverão estar contempladas, no mínimo, as seguintes atividades, referentes à solução objeto do contrato, acompanhamento de chamados junto ao fabricante:

14.235.1.1. Abertura, acompanhamento e encerramento de chamados técnicos junto ao fabricante da solução, sempre que necessário suporte de 3º nível;

14.235.1.2. Tradução, quando necessário, das recomendações do fabricante para linguagem técnica compreensível pela equipe da CONTRATANTE;

14.235.1.3. Garantia de que as correções e recomendações aprovadas sejam devidamente implementadas no ambiente da CONTRATANTE.

14.235.2. Configuração e revisão de políticas:

14.235.2.1. Configuração de novas políticas de segurança, monitoramento ou resposta, após análise de requisitos e aceite da CONTRATANTE;

14.235.2.2. Revisão periódica das políticas já existentes, com base em incidentes ocorridos, recomendações do fabricante e boas práticas.

14.235.3. Atualização de versão e novas funcionalidades:

14.235.3.1. Planejamento e execução de atualizações de versão da solução, incluindo testes preliminares, aplicação em ambiente de produção e acompanhamento pós-implantação;

14.235.3.2. Implementação de novas funcionalidades disponibilizadas pelo fabricante, quando aderentes ao escopo contratado e aprovadas pela CONTRATANTE.

14.235.4. Atendimento a dúvidas e ações corretivas/evolutivas:

14.235.4.1. Esclarecimento de dúvidas operacionais e técnicas da equipe da CONTRATANTE;

14.235.4.2. Execução de ações corretivas (correção de falhas, erros de configuração, mau funcionamento) e ações evolutivas (melhorias, otimizações, inclusão de novos cenários de uso), desde que dentro do escopo da solução contratada.

14.235.5. Relatórios de incidentes e auditoria:

14.235.5.1. Elaboração e disponibilização de relatórios de incidentes e relatórios de auditoria, com base nas informações geradas pela plataforma;

14.235.5.2. Observância da periodicidade, nível de detalhe e formato definidos pela CONTRATANTE;

14.235.5.3. Destaque para causas, impactos, ações tomadas e recomendações de melhoria.

14.235.6. Tratamento de falhas em agentes, sensores e políticas:

14.235.6.1. Análise e tratamento de falhas de instalação, comunicação ou funcionamento dos agentes ou sensores da solução;

14.235.6.2. Correção de falhas nas políticas de proteção e resposta, incluindo ajustes que se façam necessários para restabelecer o nível adequado de segurança e operação.

14.235.7. Análise e tratamento de serviços indisponíveis:

14.235.7.1. Identificação de indisponibilidades relacionadas à solução (ex.: console de gestão, módulos de coleta, serviços de correlação ou resposta);

14.235.7.2. Adoção de medidas de diagnóstico, correção e, quando cabível, escalonamento ao fabricante;

14.235.7.3. Registro das ações realizadas e dos tempos de indisponibilidade, para fins de acompanhamento de SLA.

14.235.8. Suporte às equipes internas:

14.235.8.1. Suporte técnico às equipes de cibersegurança, infraestrutura, atendimento e demais áreas correlatas da CONTRATANTE, para integração da solução com o ambiente existente;

14.235.8.2. Apoio na interpretação de alertas, eventos e relatórios gerados pela solução.

14.235.9. Suporte à instalação de novos agentes de segurança:

14.235.9.1. Apoio à instalação e configuração de novos agentes, sensores ou componentes de software necessários à expansão da solução, de acordo com o crescimento do parque ou com novos requisitos de segurança definidos pela CONTRATANTE;

14.235.9.2. Orientação quanto a pré-requisitos, compatibilidade e melhores práticas de implantação.

Sistema Zero Trust (Confiança Zero), Microsegmentação e Ofuscação

14.236. O serviço de operação assistida para o Sistema Zero Trust (Confiança Zero), Microsegmentação e Ofuscação tem por objetivo garantir a manutenção contínua, o ajuste fino e a evolução operacional dos controles de segurança associados a esses componentes, assegurando que os princípios de Zero Trust estejam efetivamente implementados, monitorados e aprimorados ao longo de toda a vigência contratual, e não apenas na fase de implantação inicial;

14.237. Objetivos do Serviço de Operação Assistida:

14.237.1. **Fortalecimento contínuo da postura de segurança Zero Trust** Assegurar que os princípios de Zero Trust – verificar explicitamente, conceder acesso mínimo (least privilege) e assumir violação como hipótese de trabalho – sejam continuamente aplicados, monitorados e revisados, garantindo que:

14.237.1.1. As políticas de autenticação, autorização e verificação de identidade estejam coerentes com o risco e o contexto de acesso;

14.237.1.2. As regras de acesso a aplicações, serviços e dados sejam constantemente reavaliadas à luz de mudanças de ambiente, usuários e ameaças;

14.237.1.3. Haja mecanismos operacionais para detectar e tratar desvios em relação ao modelo de confiança zero.

14.237.2. Prevenção e mitigação proativa de ransomware e outras ameaças avançadas deverá operar e ajustar, de forma contínua, as camadas de segurança relacionadas a Zero Trust e microsegmentação, visando:

14.237.2.1. Detectar e bloquear tentativas de infecção por ransomware e malware avançado;

14.237.2.2. Reduzir a movimentação lateral por meio de segmentação granular de rede e cargas de trabalho;

14.237.2.3. Mitigar tentativas de elevação de privilégio e uso indevido de credenciais;

14.237.2.4. Restringir ou impedir criptografia não autorizada de dados em sistemas e segmentos críticos.

14.237.3. Otimização permanente da microssegmentação deverá revisar e ajustar periodicamente as políticas de microsegmentação, garantindo que:

14.237.3.1. As regras reflitam a realidade atual da arquitetura de aplicações e serviços (incluindo ambientes on-premises e nuvem);

14.237.3.2. Não haja impacto indevido em operações legítimas, minimizando falsos bloqueios;

14.237.3.3. O desenho de segmentação acompanhe mudanças de infraestrutura, novos sistemas e desativações de serviços.

14.237.4. **Gestão da superfície de ataque e vulnerabilidades com apoio da ofuscação deverá** manter a ofuscação de ativos (por exemplo, mascaramento de portas/serviços, camuflagem de respostas, redução de informações expostas) ativa e eficaz, e:

14.237.4.1. Correlacionar achados de exposição de ativos com o roadmap de vulnerabilidades da CONTRATANTE;

14.237.4.2. Apoiar a priorização de ações de remediação com base em risco, criticidade e facilidade de exploração;

14.237.4.3. Contribuir para a redução da superfície de ataque observável por agentes maliciosos.

14.237.5. Conformidade e governança em segurança Zero Trust deverão gerar e manter evidências operacionais mensais que demonstrem:

14.237.5.1. A efetividade dos controles implementados;

14.237.5.2. A aderência aos frameworks de referência (NIST CSF, CIS Controls, ISO/IEC 27001, entre outros);

14.237.5.3. O apoio às exigências legais e regulatórias aplicáveis, incluindo, mas não se limitando à Lei Geral de Proteção de Dados – LGPD.

14.238. Manutenção operacional do Sistema Zero Trust:

14.238.1. A CONTRATADA deverá apoiar na operaçao em conjunto com a equipe da CONTRATANTE, os componentes da arquitetura Zero Trust, incluindo:

14.238.1.1. Mecanismos de autenticação forte e verificação contínua (ex.: MFA, verificação baseada em risco);

14.238.1.2. Políticas de acesso condicional e controle de sessão;

14.238.1.3. Regras de acesso baseadas em identidade, contexto e postura de segurança dos dispositivos.

14.238.2. Deverá realizar, periodicamente:

14.238.2.1. Revisão de perfis de acesso e grupos de privilégio;

14.238.2.2. Ajustes em políticas de acesso mínimo, com base em incidentes, auditorias e mudanças organizacionais;

14.238.2.3. Validação da aderência das políticas de Zero Trust às diretrizes internas de segurança e às recomendações do fabricante.

14.239. Operação e otimização da microssegmentação:

14.239.1. A CONTRATADA deverá realizar e manter:

14.239.1.1. Configurar, revisar e ajustar segmentações de rede e de cargas de trabalho, alinhadas à criticidade dos sistemas e dados;

14.239.1.2. Apoiar a definição e manutenção de zonas de segurança e políticas de comunicação permitida entre segmentos (east-west traffic);

14.239.1.3. Documentação atualizada da arquitetura de microsegmentação (mapas de fluxo de comunicação, regras principais, exceções);

14.239.1.4. Processos padronizados para solicitação, aprovação e revisão de exceções de comunicação.

14.240. Manutenção da ofuscação de ativos:

14.240.1. A CONTRATADA deverá:

14.240.1.1. Apoiar a operação dos mecanismos de ofuscação (por exemplo, ocultação de portas/serviços, respostas enganosas controladas, limitação de banners e informações de sistema);

14.240.1.2. Avaliar, com periodicidade definida, a efetividade da ofuscação na redução de informações expostas a scans e tentativas de reconhecimento (reconnaissance).

14.240.2. Deverá correlacionar:

14.240.2.1. Achados de scans e tentativas de reconhecimento malicioso com os controles de ofuscação;

14.240.2.2. Resultados de ofuscação com a priorização de correções em vulnerabilidades, configurando a solução de forma a dificultar mapeamento de ativos por atacantes.

Serviço de Operação Assistida e treinamento para a solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall (NGFW), composta pelos equipamentos Modelos I, II, II e IV deste Termo de Referência

14.241. Objetivo:

14.241.1. Prestação de serviço gerenciado mensal de operação assistida, monitoramento contínuo e resposta a incidentes de segurança, para a solução de proteção de perímetro de rede lógica do tipo Next Generation Firewall (NGFW), composta pelos equipamentos Modelos I, II, II e IV deste Termo de Referência, incluindo gerenciamento centralizado, atualização de assinaturas, aplicação de contramedidas e notificação de tentativas de invasão, pelo período de 12 meses.

14.242. Escopo do serviço:

14.242.1. Abrangência:

14.242.1.1. O serviço de operação assistida abrangerá todos os equipamentos fornecidos no âmbito desta contratação, incluindo;

14.242.1.2. Firewalls instalados na sede, data center e unidades descentralizadas;

14.242.1.3. Plataforma de gerenciamento centralizado (Network Security Manager);

14.242.1.4. Sistemas de logging, monitoramento e alertas;

14.242.1.5. Infraestrutura de conectividade associada à solução de segurança contratada.

14.243. Modalidade de execução:

14.243.1. O serviço de operação assistida poderá ser executado de forma:

14.243.1.1. Presencial, quando demandar intervenção física nos equipamentos ou na infraestrutura local; ou

14.243.1.2. Remota, mediante autorização expressa do órgão contratante e observância de sua Política de Segurança da Informação, com avaliação dos riscos envolvidos em acessos externos.

14.243.2. Horários e regimes:

14.243.2.1. Regime de atuação da equipe técnica para gerenciamento e configuração, das 8h às 18h em dias úteis (8x5), com regime de sobreaviso para incidentes críticos fora desse horário;

14.243.2.2. Regime de resposta a incidentes críticos, durante 24x7, com tempo máximo de resposta conforme SLA definido;

14.243.2.3. Regime de Serviços programados (atualizações, mudanças), em dias úteis, das 8h às 18h, com janela previamente aprovada pelo contratante.

14.244. Descrição detalhada das atividades mensais:

14.244.1. Atividades contínuas (diárias):

14.244.1.1. **Monitoramento de disponibilidade**: verificação contínua do status operacional de todos os equipamentos, interfaces, túneis VPN e serviços de segurança;

14.244.1.2. **Monitoramento de desempenho**: acompanhamento de CPU, memória, conexões simultâneas, throughput e utilização das interfaces em todos os equipamentos;

14.244.1.3. **Análise de logs e eventos**: coleta, correlação e análise dos registros de segurança gerados pelos firewalls, incluindo eventos de IPS, antimalware, controle de aplicações, filtragem web e inspeção TLS/SSL;

14.244.1.4. **Detecção e notificação de incidentes**: identificação de tentativas de invasão, ataques, infecções por malware, tráfego anômalo e violações de política, com notificação imediata ao contratante;

14.244.1.5. **Aplicação de contramedidas**: bloqueio automático ou manual de ameaças identificadas, isolamento de endpoints comprometidos e atualização de regras de bloqueio;

14.244.1.6. **Verificação de licenças e assinaturas**: monitoramento da validade das licenças, subscrições e assinaturas de segurança, com alerta preventivo de expiração.

14.244.2. Atividades semanais:

14.244.2.1. **Revisão de regras de firewall**: análise das regras ativas, inativas, não utilizadas e redundantes, com recomendação de otimização;

14.244.2.2. **Verificação de atualizações**: conferência de novas versões de firmware, assinaturas de IPS, antimalware e inteligência de ameaças disponibilizadas pelo fabricante;

14.244.2.3. **Teste de conectividade**: verificação dos túneis VPN site-to-site e de acesso remoto, incluindo testes de throughput e latência;

14.244.2.4. **Revisão de logs de administração**: auditoria dos acessos administrativos, alterações de configuração e tentativas de autenticação mal sucedidas;

14.244.2.5. **Backup de configuração**: verificação e validação dos backups automáticos e manuais das configurações de todos os equipamentos.

14.244.3. Atividades mensais:

14.244.3.1. **Relatório gerencial mensal**: elaboração e entrega de relatório consolidado contendo:

14.244.3.1.1. Disponibilidade dos equipamentos e serviços;

14.244.3.1.2. Utilização de recursos (CPU, memória, conexões, throughput);

14.244.3.1.3. Estatísticas de ameaças detectadas e bloqueadas;

14.244.3.1.4. Incidentes de segurança registrados e tratados;

14.244.3.1.5. Principais aplicações e categorias de tráfego;

14.244.3.1.6. Consumo de banda por aplicação, usuário e unidade;

14.244.3.1.7. Alterações de configuração realizadas;

14.244.3.1.8. Recomendações de melhoria e otimização;

14.244.3.1.9. Projeção de capacidade e necessidades futuras.

14.244.3.2. **Reunião de acompanhamento**: realização de reunião mensal com o gestor do contrato para apresentação dos resultados, discussão de ocorrências e planejamento de atividades;

14.244.3.3. **Atualização programada de firmware e assinaturas**: aplicação de atualizações críticas e recomendadas, em janela previamente aprovada, com plano de rollback documentado;

14.244.3.4. **Teste de failover e continuidade**: execução de teste controlado de failover de links, alta disponibilidade e conectividade celular, quando aplicável;

14.244.3.5. **Revisão de políticas de segurança**: análise e recomendação de ajustes nas políticas de firewall, IPS, controle de aplicações, filtragem web e VPN, com base no comportamento observado e nas ameaças emergentes;

14.244.3.6. **Gestão de capacidade**: avaliação da utilização atual versus capacidade máxima dos equipamentos, com projeção de crescimento e recomendação de upgrade quando necessário

14.244.4. Atividades trimestrais:

14.244.4.1. **Relatório de capacidade**: entrega de relatório detalhado de capacidade operacional, contendo dados consolidados de utilização de recursos e projeções de necessidades futuras, conforme previsto na Consulta Pública nº 09/2025.

14.244.5. Atividades anuais:

14.244.5.1. **Revisão geral de arquitetura**: análise completa da arquitetura de segurança, incluindo topologia, segmentação, políticas e integração com sistemas externos;

14.244.5.2. **Simulação de desastre**: execução de simulação completa de falha e recuperação, incluindo restauração a partir de backup, failover entre equipamentos e comutação para link secundário;

14.244.5.3. **Plano de evolução tecnológica**: elaboração de plano de evolução tecnológica para o período seguinte, considerando fim de vida dos equipamentos, novas ameaças e necessidades institucionais.

14.245. Procedimentos de contingência:

14.245.1. **Escalonamento de incidentes**: definição de níveis de criticidade e cadeia de escalonamento com tempos máximos de resposta e resolução para cada nível;

14.245.2. **Equipe de sobreaviso**: disponibilização de equipe técnica certificada em regime de sobreaviso 24x7 para incidentes críticos, com tempo máximo de resposta de **15 minutos** para acionamento e **2 horas** para início da atuação;

14.245.3. **Plano de continuidade**: procedimentos documentados para failover entre equipamentos, comutação para link secundário, restauração de backup e acionamento de conectividade celular;

14.245.4. **Comunicação de incidentes**: protocolo de comunicação com o contratante, incluindo notificação inicial, atualizações periódicas e relatório final de encerramento do incidente;

14.245.5. **Suporte do fabricante**: acesso direto ao suporte técnico do fabricante, com acionamento de casos críticos e acompanhamento até a resolução.

14.246. Métricas de sucesso e critérios de avaliação:

14.246.1. Indicadores de desempenho (KPIs):

Indicador	Descrição	Meta mensal	Forma de medição
Disponibilidade da solução	Percentual de tempo em que todos os firewalls e serviços de segurança estiveram operacionais	≥ 99,5%	Monitoramento 24x7, relatório de uptime
Tempo médio de resposta (TMR)	Tempo entre a abertura do chamado e o primeiro contato da equipe técnica	≤ 15 minutos (crítico) / ≤ 1 hora (alto) / ≤ 4 horas (médio) / ≤ 8 horas (baixo)	Registro no sistema de tickets
Tempo médio de resolução (TMRs)	Tempo entre a abertura do chamado e a resolução definitiva	≤ 4 horas (crítico) / ≤ 8 horas (alto) / ≤ 24 horas (médio) / ≤ 72 horas (baixo)	Registro no sistema de tickets
Eficácia de bloqueio de ameaças	Percentual de ameaças conhecidas bloqueadas automaticamente pela solução	≥ 98%	Relatório mensal de ameaças
Atualização de assinaturas	Percentual de assinaturas atualizadas dentro do prazo recomendado pelo fabricante	100%	Verificação semanal do status de atualização
Backup de configuração	Percentual de backups realizados e validados com sucesso	100%	Verificação semanal de integridade dos backups
Entrega de relatórios	Percentual de relatórios mensais entregues dentro do prazo acordado	100%	Registro de entrega e protocolo
Satisfação do contratante	Avaliação qualitativa do serviço pelo gestor do contrato	≥ 80% de satisfação	Pesquisa mensal de satisfação
Tempo de execução de mudanças programadas	Cumprimento das janelas de mudança aprovadas	≥ 95% de cumprimento	Comparação entre janela planejada e execução real
Índice de reincidência	Percentual de incidentes que se repetem em um período de 30 dias	≤ 5%	Análise de tickets e relatórios de incidentes

14.247. Critérios de avaliação do desempenho:

14.247.1. O desempenho do serviço de operação assistida será avaliado mensalmente com base nos seguintes critérios:

14.247.1.1. **Cumprimento dos SLAs**: todos os indicadores deverão atender às metas estabelecidas. O descumprimento reiterado de qualquer indicador poderá implicar em glosa no pagamento mensal e aplicação de sanções contratuais;

14.247.1.2. **Qualidade dos relatórios**: os relatórios mensais, trimestrais e anuais deverão ser claros, objetivos, tecnicamente consistentes e conter todas as informações estabelecidas neste Termo de Referência;

14.247.1.3. **Tempestividade nas comunicações**: incidentes críticos deverão ser comunicados imediatamente ao gestor do contrato, independentemente do horário. Atrasos na comunicação de incidentes críticos serão considerados falha grave;

14.247.1.4. **Proatividade**: a contratada deverá demonstrar postura proativa na identificação de riscos, recomendação de melhorias e otimização da solução, não se limitando à atuação reativa;

14.247.1.5. **Documentação**: toda atividade relevante deverá ser documentada, incluindo procedimentos executados, mudanças realizadas, incidentes tratados e recomendações emitidas.

14.248. A CONTRATADA deverá:

14.248.1. Comunicar previamente qualquer alteração na composição da equipe técnica alocada ao contrato;

14.248.2. Fornecer substituição imediata de profissional que não atenda aos requisitos técnicos ou cuja atuação seja considerada insatisfatória pelo contratante;

14.248.3. Manter inventário atualizado de todos os equipamentos, licenças e configurações sob sua gestão;

14.248.4. Cumprir integralmente a Política de Segurança da Informação do contratante e a LGPD.

Serviço de Operação Assistida e treinamento para a solução de à plataforma de anonimização, executados sob demanda e remunerados por Unidade de Serviço Técnico (UST), deste Termo de Referência

14.249. Compreende a prestação de serviços técnicos especializados para implantação, integrações, customizações e consultoria relacionados à plataforma de anonimização, executados sob demanda e remunerados por Unidade de Serviço Técnico (UST);

14.250. A Unidade de Serviço Técnico (UST) corresponde a 1 (uma) hora de trabalho de profissional de nível sênior, sendo utilizada como métrica para mensuração e pagamento dos serviços técnicos especializados;

14.251. Os serviços técnicos compreendem, de forma não exaustiva:

14.251.1. Implantação e configuração inicial da plataforma no ambiente do CONTRATANTE;

14.251.2. Integração com sistemas corporativos (SEI, GED, portais de transparência, sistemas de autenticação);

14.251.3. Customização de funcionalidades para atendimento a requisitos específicos;

14.251.4. Consultoria em proteção de dados pessoais e conformidade LGPD;

14.251.5. Elaboração de Relatório de Impacto à Proteção de Dados Pessoais (RIPD);

14.251.6. Apoio técnico ao Encarregado de Dados (DPO) do órgão;

14.251.7. Assessoria na resposta a incidentes de segurança e demandas da ANPD.

15. MODELO DE EXECUÇÃO DO CONTRATO

Condições de execução

15.1. A execução do objeto seguirá a seguinte dinâmica:

15.1.1. A contratada deverá iniciar o desenvolvimento dos módulos no prazo máximo de **7 (sete) dias**, contados da assinatura do contrato, devendo disponibilizar a software plenamente operacional no prazo de até **90 (noventa) dias**, também contados da assinatura do instrumento contratual;

15.1.2. Todo o processo de desenvolvimento e implantação da solução será acompanhado e supervisionado pela Contratante.

Suporte e Manutenção

15.2. A CONTRATADA deverá manter o serviço de suporte técnico para todos os itens deste Termo de Referência disponível 8 (oito) horas por dia, 5 (cinco) dias por semana, exceto nos períodos destinados a manutenção programada;

15.3. A severidade do problema/incidente será informada pela CONTRANTE, de acordo com os critérios da ocorrência, conforme classificação descritos na tabela de suporte técnico definida abaixo;

15.4. De acordo com a classificação da severidade, a CONTRATADA deverá cumprir os prazos conforme classificação descrita na tabela de SLA abaixo;

15.5. Entende-se por Retorno à Operação o tempo decorrido entre o início do chamado técnico e o encaminhamento da solução;

15.6. Deverá ser disponibilizado um canal de comunicação para contato de suporte técnico para o caso de bug/problemas técnicos, bem como indisponibilidade do ambiente ou questões referentes à taxa de atualização;

15.7. A abertura de chamados poderá ser feita pelos administradores do sistema da CONTRANTE, ou diretamente pelos usuários. Se o chamado encaminhado não estiver relacionado a dúvidas na operação do serviço, eles deverão orientar o solicitante a encaminhar a demanda ao suporte operacional;

15.8. Um chamado técnico somente poderá ser considerado encerrado após confirmação do responsável indicado pela CONTRANTE, e o término do atendimento se dará com a disponibilidade do serviço para uso em perfeitas condições de funcionamento no local onde estiver instalado;

15.9. Caso o chamado não se refira ao objeto deste termo de referência, ou ainda, por falta de elementos essenciais ao seu entendimento, a CONTRATADA deverá comunicar formalmente a CONTRANTE, acerca do encerramento do chamado, apresentando a respectiva justificativa, ou solicitar informações complementares para resolução do chamado;

15.10. Atualização A CONTRATADA deverá manter a(s) soluçao(oes) atualizada(s) e compatível(eis) com as novas versões e atualizações dos sistemas operacionais, componentes e navegadores que forem lançados durante a vigência do contrato;

15.11. A CONTRATADA deverá prestar os serviços de suporte e manutenção contínuos, durante a vigência do contrato, da(s) soluçao(oes). Este serviço visa garantir o funcionamento ininterrupto da(s) soluçao(oes) e a atualização constante de suas funcionalidades e a pronta assistência para quaisquer questões técnicas ou operacionais que possam surgir, deverão atender aos seguintes requisitos:

15.11.1. Atendimento a Incidentes: Suporte ágil para resolução de problemas técnicos, erros ou falhas na plataforma, com tempos de resposta definidos em SLA (Service Level Agreement);

15.11.2. Dúvidas e Orientações de Uso: Esclarecimento de dúvidas sobre as funcionalidades da plataforma, auxílio na interpretação de relatórios e orientações para o uso otimizado dos recursos;

15.11.3. Canais de Comunicação: Disponibilidade de canal de suporte via telefone ou e-mail para facilitar a comunicação e agilizar o atendimento;

15.11.4. Atualizações de Software: Garantia de que a plataforma esteja sempre com as versões mais recentes, incluindo correções de bugs, melhorias de desempenho e novas funcionalidades;

15.11.5. Ajustes e Otimizações: Realização de ajustes e otimizações na configuração da plataforma para assegurar que ela opere com máxima eficiência e performance, adaptando-se às necessidades da sua infraestrutura;

15.11.6. Gestão de Integrações: Manutenção das integrações com outras ferramentas de segurança da informação, garantindo que o fluxo de dados e informações seja contínuo e sem interrupções;

15.11.7. Melhoria Contínua: A plataforma deve evoluir para incorporar novas tecnologias e atender às futuras demandas do mercado de segurança da informação;

15.11.8. Verificação de Saúde: Monitoramento proativo da saúde e integridade dos componentes da plataforma, identificando potenciais gargalos ou falhas antes que impactem a operação;

15.11.9. Otimização de Banco de Dados: Manutenção e otimização do banco de dados da plataforma para garantir a agilidade na recuperação e análise das informações de risco e conformidade.

15.12. O processo ocorrerá da seguinte forma:

15.12.1. Prévia análise das necessidades pela CONTRANTE e CONTRATADA;

15.12.2. Caso seja um desenvolvimento já previsto neste Termo de Referência, a manutenção não deverá incorrer em ônus à CONTRATANTE;

15.12.3. Quaisquer alterações e ou manutenções, bem como, o pagamento pelos serviços prestados (quando houver), estarão condicionados à homologação por parte da Contratante bem como ao fornecimento de documentação atualizada técnica e funcional.

16. MODELO DE GESTÃO DO CONTRATO

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

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

16.3. As comunicações entre o órgão ou entidade e a contratada devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim;

16.4. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato;

16.5. Após a assinatura do contrato ou instrumento equivalente, o órgão ou entidade poderá convocar o representante da empresa contratada para reunião inicial para apresentação do plano de fiscalização, que conterá informações acerca das obrigações contratuais, dos mecanismos de fiscalização, das estratégias para execução do objeto, do plano complementar de execução da contratada, quando houver, do método de aferição dos resultados e das sanções aplicáveis, dentre outros.

Fiscalização

16.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput) , nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

16.7. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

16.7.1. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

16.7.2. Identificada qualquer inexatidão ou irregularidade, o fiscal técnico do contrato emitirá notificações para a correção da execução do contrato, determinando prazo para a correção. (Decreto nº 11.246, de 2022, art. 22, III);

16.7.3. O fiscal técnico do contrato informará ao gestor do contato, em tempo hábil, a situação que demandar decisão ou adoção de medidas que ultrapassem sua competência, para que adote as medidas necessárias e saneadoras, se for o caso. (Decreto nº 11.246, de 2022, art. 22, IV);

16.7.4. No caso de ocorrências que possam inviabilizar a execução do contrato nas datas aprazadas, o fiscal técnico do contrato comunicará o fato imediatamente ao gestor do contrato. (Decreto nº 11.246, de 2022, art. 22, V);

16.7.5. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à renovação tempestiva ou à prorrogação contratual (Decreto nº 11.246, de 2022, art. 22, VII).

Fiscalização Administrativa

16.8. O fiscal administrativo do contrato, além de exercer as atribuições previstas no art. 33, IV, da IN SGD nº 94, de 2022, verificará a manutenção das condições de habilitação do contratado, acompanhará o empenho, o pagamento, as garantias, as glosas e a formalização de apostilamento e termos aditivos, solicitando quaisquer documentos comprobatórios pertinentes, caso necessário (Art. 23, I e II, do Decreto nº 11.246, de 2022).

16.8.1. Caso ocorra descumprimento das obrigações contratuais, o fiscal administrativo do contrato atuará tempestivamente na solução do problema, reportando ao gestor do contrato para que tome as providências cabíveis, quando ultrapassar a sua competência; (Decreto nº 11.246, de 2022, art. 23, IV).

Gestor do Contrato

16.9. O gestor do contrato, além de exercer as atribuições previstas no art. 33, I, da IN SGD nº 94, de 2022, coordenará a atualização do processo de acompanhamento e fiscalização do contrato contendo todos os registros formais da execução no histórico de gerenciamento do contrato, a exemplo da ordem de serviço, do registro de ocorrências, das alterações e das prorrogações contratuais, elaborando relatório com vistas à verificação da necessidade de adequações do contrato para fins de atendimento da finalidade da administração. (Decreto nº 11.246, de 2022, art. 21, IV);

16.10. O gestor do contrato acompanhará os registros realizados pelos fiscais do contrato, de todas as ocorrências relacionadas à execução do contrato e as medidas adotadas, informando, se for o caso, à autoridade superior àquelas que ultrapassarem a sua competência. (Decreto nº 11.246, de 2022, art. 21, II);

16.11. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III);

16.12. O gestor do contrato emitirá documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial quanto ao cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado nos indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações. (Decreto nº 11.246, de 2022, art. 21, VIII);

16.13. O gestor do contrato tomará providências para a formalização de processo administrativo de responsabilização para fins de aplicação de sanções, a ser conduzido pela comissão de que trata o art. 158 da

Lei nº 14.133, de 2021, ou pelo agente ou pelo setor com competência para tal, conforme o caso. (Decreto nº 11.246, de 2022, art. 21, X);

16.14. O gestor do contrato deverá elaborará relatório final com informações sobre a consecução dos objetivos que tenham justificado a contratação e eventuais condutas a serem adotadas para o aprimoramento das atividades da Administração. (Decreto nº 11.246, de 2022, art. 21, VI);

16.15. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

17. CRITÉRIOS DE RECEBIMENTO E PAGAMENTO

Dos recebimentos dos serviços

17.1. O serviço de serão recebidos provisoriamente, no prazo de 10 (dez) dias, pelos fiscais técnico e/ou administrativo, mediante termos detalhados, quando verificado o cumprimento das exigências de caráter técnico e administrativo;

17.2. O prazo para recebimento provisório será contado do recebimento de comunicação da finalização do serviço de implementação pela empresa;

17.3. O fiscal técnico/ou administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter técnico. (Art. 22, X, Decreto nº 11.246, de 2022);

17.4. O fiscal administrativo do contrato realizará o recebimento provisório do objeto do contrato mediante termo detalhado que comprove o cumprimento das exigências de caráter administrativo. (Art. 23, X, Decreto nº 11.246, de 2022);

17.5. O fiscal setorial do contrato, quando houver, realizará o recebimento provisório sob o ponto de vista técnico e administrativo;

17.5.1. Será considerado como ocorrido o recebimento provisório com a entrega do termo detalhado ou, em havendo mais de um a ser feito, com a entrega do último.

17.6. O Contratado fica obrigado a reparar, corrigir, remover, reconstruir ou substituir, às suas expensas, no todo ou em parte, o objeto em que se verificarem vícios, defeitos ou incorreções resultantes da execução ou materiais empregados, cabendo à fiscalização não atestar a última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório;

17.7. A fiscalização não efetuará o ateste da última e/ou única medição de serviços até que sejam sanadas todas as eventuais pendências que possam vir a ser apontadas no Recebimento Provisório. (Art. 119 c/c art. 140 da Lei nº 14133, de 2021);

17.8. O recebimento provisório também ficará sujeito, quando cabível, à conclusão de todos os testes de campo e à entrega dos Manuais e Instruções exigíveis;

17.9. Os serviços poderão ser rejeitados, no todo ou em parte, quando em desacordo com as especificações constantes neste Termo de Referência e na proposta, sem prejuízo da aplicação das penalidades;

17.10. Quando a fiscalização for exercida por um único servidor, o Termo Detalhado deverá conter o registro, a análise e a conclusão acerca das ocorrências na execução do contrato, em relação à fiscalização técnica e administrativa e demais documentos que julgar necessários, devendo encaminhá-los ao gestor do contrato para recebimento definitivo;

17.11. Os serviços serão recebidos definitivamente no prazo de até 10 (dez) dias corridos, contatos do contados do recebimento provisório, por servidor ou comissão designada pela autoridade competente, após a verificação da qualidade e quantidade do serviço e consequente aceitação mediante termo detalhado, obedecendo os seguintes procedimentos:

17.11.1. Emitir documento comprobatório da avaliação realizada pelos fiscais técnico, administrativo e setorial, quando houver, no cumprimento de obrigações assumidas pelo contratado, com menção ao seu desempenho na execução contratual, baseado em indicadores objetivamente definidos e aferidos, e a eventuais penalidades aplicadas, devendo constar do cadastro de atesto de cumprimento de obrigações, conforme regulamento (art. 21, VIII, Decreto nº 11.246, de 2022);

17.11.2. Realizar a análise dos relatórios e de toda a documentação apresentada pela fiscalização e, caso haja irregularidades que impeçam a liquidação e o pagamento da despesa, indicar as cláusulas contratuais pertinentes, solicitando à Contratada, por escrito, as respectivas correções;

17.11.3. Emitir Termo Detalhado para efeito de recebimento definitivo dos serviços prestados, com base nos relatórios e documentações apresentadas;

17.11.4. Comunicar a empresa para que emita a Nota Fiscal ou Fatura, com o valor exato dimensionado pela fiscalização; e

17.11.5. Enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão.

17.12. No caso de controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, deverá ser observado o teor do art. 143 da Lei nº 14.133, de 2021, comunicando-se à empresa para emissão de Nota Fiscal no que concerne à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento;

17.13. Nenhum prazo de recebimento ocorrerá enquanto pendente a solução, pelo contratado, de inconsistências verificadas na execução do objeto ou no instrumento de cobrança;

17.14. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança do serviço nem a responsabilidade ético-profissional pela perfeita execução do contrato.

Liquidação

17.15. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de dez dias úteis para fins de liquidação, na forma desta seção, prorrogáveis por igual período, nos termos do art. 7º, §2º da Instrução Normativa SEGES/ME nº 77/2022;

17.16. O prazo de que trata o item anterior será reduzido à metade, mantendo-se a possibilidade de prorrogação, no caso de contratações decorrentes de despesas cujos valores não ultrapassem o limite de que trata o inciso II do art. 75 da Lei nº 14.133, de 2021;

17.17. Para fins de liquidação, o setor competente deverá verificar se a nota fiscal ou instrumento de cobrança equivalente apresentado expressa os elementos necessários e essenciais do documento, tais como:

17.17.1. o prazo de validade;

17.17.2. a data da emissão;

17.17.3. os dados do contrato e do órgão contratante;

17.17.4. o período respectivo de execução do contrato;

17.17.5. descrição do serviço prestado;

17.17.6. o valor a pagar; e

17.17.7. eventual destaque do valor de retenções tributárias cabíveis.

17.18. Havendo erro na apresentação da nota fiscal ou instrumento de cobrança equivalente, ou circunstância que impeça a liquidação da despesa, esta ficará sobrestada até que o contratado providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao contratante;

17.19. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no art. 68 da Lei nº 14.133, de 2021;

17.20. A Administração deverá realizar consulta para:

17.20.1. Verificar a manutenção das condições de habilitação exigidas no edital;

17.20.2. Identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE2018).

17.21. Constatando-se a situação de irregularidade do contratado, será providenciada sua notificação, por escrito, para que, no prazo de 5 (cinco) dias úteis, regularize sua situação ou, no mesmo prazo, apresente sua defesa. O prazo poderá ser prorrogado uma vez, por igual período, a critério do contratante;

17.22. Não havendo regularização ou sendo a defesa considerada improcedente, o contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência do contratado, bem como quanto à existência de pagamento a ser efetuado, para que sejam acionados os meios pertinentes e necessários para garantir o recebimento de seus créditos;

17.23. Persistindo a irregularidade, o contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada ao contratado a ampla defesa;

17.24. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso o contratado não regularize sua situação junto ao SICAF.

Prazo de pagamento

17.25. O pagamento pelos serviços prestados será efetuado até o dia 10 (dez) do do recebimento definitivo da prestação dos serviços, à vista das notas fiscais decorrentes ou outros documentos equivalentes, em conformidade com a seção anterior, nos termos da Instrução Normativa SEGES/ME nº 77, de 2022;

17.26. No caso de atraso pelo Contratante, os valores devidos ao contratado serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do índice IPCA-E de correção monetária.

Forma de pagamento

17.27. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo contratado;

17.28. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento;

17.29. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável;

17.30. Independentemente do percentual de tributo inserido na planilha, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente;

17.31. O contratado regularmente optante pelo Simples Nacional, nos termos da Lei Complementar nº 123, de 2006, não sofrerá a retenção tributária quanto aos impostos e contribuições abrangidos por aquele regime. No entanto, o pagamento ficará condicionado à apresentação de comprovação, por meio de documento oficial, de que faz jus ao tratamento tributário favorecido previsto na referida Lei Complementar.

18. PAPÉIS E RESPONSABILIDADES

18.1. São obrigações da CONTRATANTE:

18.1.1. receber, fiscalizar, orientar, contestar, dirimir dúvidas emergentes da execução do objeto contratado;

18.1.2. nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;

18.1.3. encaminhar formalmente a demanda por meio de Ordem de Serviço ou Autorização de Fornecimento, de acordo com os critérios estabelecidos no Termo de Referência;

18.1.4. receber o serviço prestado pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

18.1.5. notificar a contrata, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele reparado ou corrigido, no total ou em parte, às suas expensas

18.1.6. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;

18.1.7. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;

18.1.8. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução;

18.1.9. resguardar os direitos de propriedade intelectual e direitos autorais da solução sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;

18.1.10. fornecer à Contratada todas as informações, os esclarecimentos, os documentos e as demais condições necessárias à execução do contrato;

18.1.11. zelar para que sejam cumpridas as obrigações assumidas pela licitante vencedora e para que sejam mantidas todas as condições de habitação e qualificação exigidas na licitação.

18.2. São obrigações do CONTRATADA:

18.2.1. indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;

18.2.2. assumir a responsabilidade pela prestação dos serviços descritos neste Termo de Referência, no Edital e no Contrato, inclusive fornecer o serviço licitado tomando especial cuidado para que os módulos sejam aqueles atendam as especificações técnicas constante neste Termo;

18.2.3. dar fiel execução ao objeto desta contratação, bem como providenciar às suas expensas e a contento do Contratante todas as substituições e correções que se fizerem necessárias;

18.2.4. atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

18.2.5. reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;

18.2.6. propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

18.2.7. manter, durante toda a execução do contrato, as mesmas condições da habilitação;

18.2.8. manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução;

18.2.9. não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, sem prévia anuência da contratante;

18.2.10. deverá garantir que a solução, após implementação e pleno funcionamento, estará sujeito a ajustes e alterações para atendimento de situações especificas requeridas pelo

CONTRATANTE, mediante requerimento e orçamento prévio, desde que tais alterações não interfiram na estrutura básica e demais funcionalidades;

18.2.11. dar ciência imediata e por escrito à Contratante sobre qualquer anormalidade verificada na execução dos serviços;

18.2.12. garantir que os serviços de assistência técnica, suporte, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

18.2.13. ceder os direitos de propriedade intelectual e direitos autorais da solução sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;

18.2.14. manter ciente que o armazenamento dos dados deve estar em perfeita conformidade com os ditames da Lei Federal nº 13.709, de 14 de agosto de 2018, também conhecida por Lei Geral de Proteção de Dados Pessoais (LGPD).

19. OBRIGAÇÕES PERTINENTES À LGPD

19.1. O Contratado deverá observar integralmente os requisitos de Segurança da Informação e Privacidade descritos a seguir:

19.2. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD) alterada pela Lei nº 13.853, de 2019, 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;

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

19.4. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei;

19.5. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado 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;

19.6. A CONTRATADA obriga-se a garantir a confidencialidade dos dados coletados da CONTRATANTE por meio de uma política interna de privacidade, a fim de respeitar, por si, seus funcionários e seus prepostos, o objetivo do presente termo;

19.7. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD;

19.8. Conforme prevê a Lei Geral de Proteção de Dados, obriga-se a CONTRATADA a executar os seus trabalhos e tratar os dados da CONTRATANTE respeitando os princípios da finalidade, adequação, transparência, livre acesso, segurança, prevenção e não discriminação;

19.9. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados;

19.10. Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto à eventual descarte realizado;

19.11. 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;

19.12. 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.

20. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

Forma de seleção e critério de julgamento da proposta

20.1. O fornecedor será selecionado por meio da realização de procedimento de LICITAÇÃO, na modalidade PREGÃO, sob a forma ELETRÔNICA, com adoção do critério de julgamento pelo MENOR PREÇO;

20.2. Deverá ser apresentado juntamente com a Proposta Final:

20.2.1. **DECLARAÇÃO DE QUE SUAS PROPOSTAS ECONÔMICAS COMPREENDEM A INTEGRALIDADE DOS CUSTOS** para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Exigências de habilitação

20.3. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

20.3.1. Declaração de que atende aos requisitos de habilitação, e de que o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021);

20.3.2. Declaração de Idoneidade (de que não foi declarada inidônea por ato da Administração Pública);

20.3.3. Declaração que atende ao disposto no artigo 7°, inciso XXXIII, da Constituição Federal, nos termos do inciso VI do art. 68 da Lei nº 14.133/21;

20.3.4. Declaração que não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

20.3.5. Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social;

20.3.6. Declaração da licitante de que não que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade

contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, conforme art. 14, IV da Lei nº 14.133/2021.

Declaração Exclusiva para ME/EPP:

20.4. Declaração de que cumpre os requisitos estabelecidos no artigo 3°da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos § 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021 e observância do limite de R$ 4.800.000,00 na licitação, 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.

Declaração Exclusiva Cooperativa

20.5. O licitante organizado em Cooperativa deverá apresentar declaração de que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021 (modelo em anexo).

Habilitação jurídica

20.6. **Empresário individual:** inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

20.7. **Microempreendedor Individual - MEI:** Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

20.8. **Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI**: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

20.9. **Sociedade empresária estrangeira:** portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

20.10. **Sociedade simples:** inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

20.11. **Filial, sucursal ou agência de sociedade simples ou empresária:** inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz;

20.12. **Sociedade cooperativa**: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971;

20.13. Os documentos apresentados deverão estar acompanhados de todas as alterações ou da consolidação respectiva.

Habilitação fiscal, social e trabalhista

20.14. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) atualizado, relativo ao domicílio ou sede do licitante, pertinente e compatível com o objeto desta licitação;

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

20.16. Certificado de Regularidade de Situação perante o Fundo de Garantia do Tempo de Serviço, emitido nos moldes do art. 7º, V da Lei nº 8.036, de 11 de maio de 1990;

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

20.18. Prova de inscrição no cadastro de contribuintes Municipal relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

20.19. Certidão de Regularidade com a Fazenda Municipal, relativa à atividade em cujo exercício contrata ou concorre, referente ao domicílio da sociedade empresária;

20.20. Certidão de Regularidade com a Fazenda Estadual do domicílio ou sede do licitante, dentro do prazo de validade, na forma da lei;

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

20.22. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

20.23. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II).

20.23.1. Se a Certidão de falência não estabelecer prazo de validade, será considerada válida apenas a certidão com prazo de emissão não superior a 90 (noventa) dias da data da sessão.

Qualificação Técnica

20.24. Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;

20.25. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados e/ou em execução nas seguintes áreas:

20.25.1. Operação de SOC 24x7: Comprovação de fornecimento de serviço de Security Operations Center com monitoramento contínuo, detecção avançada e resposta estendida e coordenada a incidentes;

20.25.2. Implementação e Operação de Plataforma SIEM: Experiência na implantação, tuning e operação de plataforma de correlação avançada, integrando mais de 50 fontes de dados heterogêneas;

20.25.3. Projetos de Arquitetura Zero Trust e Controle de Acesso: Implementação de soluções de ZTNA (Zero Trust Network Access);

20.25.4. Estratégia de Resiliência e Recuperação: Experiência em projetos de Backup Imutável e Disaster Recovery (DR);

20.25.5. Implantação e Operação Assistida da Plataforma de Maturidade em segurança da informação.

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

20.27. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MP n. 5, de 2017;

20.28. Os atestados ou declarações de capacidade técnica deverão se referir a serviços prestados no âmbito da atividade econômica principal e/ou secundária da licitante, especificada no contrato social devidamente registrado na junta comercial competente, bem como no cadastro de pessoas jurídicas da Receita Federal do Brasil – RFB;

20.29. Os atestados ou declarações deverão conter as seguintes informações:

20.29.1. Nome, CNPJ, dados de endereço e contato da empresa/órgão que emitiu o atestado;

20.29.2. Nome completo e cargo do signatário;

20.29.3. Descrição do serviço de modo a permitir a aferição de sua similaridade com o objeto licitado;

20.29.4. Prazo de execução e quantidade contratada (se aplicável);

20.29.5. Período e local da prestação do serviço;

20.29.6. Data de emissão do atestado;

20.29.7. Assinatura do representante do órgão atestante.

20.30. Comprovação de possuir em seu quadro permanente, na data da licitação, ou compromisso de contratação, equipe técnica multidisciplinar com profissionais das seguintes áreas:

20.30.1. 01 Analista de sistemas;

20.30.1.1. Nível superior completo em áreas da Tecnologia da Informação.

20.30.2. 01 Advogado;

20.30.2.1. Nível superior completo em direito com registro na OAB.

20.30.3. 01 Analista de requisitos;

20.30.3.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

20.30.3.2. Título de especialização em engenharia de sistemas para web, gestão empresarial ou áreas afins.

20.30.4. 01 Analista de Segurança da informação.

20.30.4.1. Nível superior completo na área de Segurança da Informação.

20.30.5. 01 Analista de Governança Corporativa.

20.30.5.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

20.30.5.2. Título de especialização em governança corporativa e risco, ou áreas afins;

20.30.5.3. Certificação Lead Assessor SIG ISO 37301:2021 – Gestão em Compliance – Requisitos com orientações para uso;

20.30.5.4. Certificação Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019 – Gestão de Riscos e Continuidade de Negócios.

20.30.6. 01 Encarregado de Dados (DPO).

20.30.6.1. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;

20.30.6.2. Certificação como Lead Assessor ISO 27001:2022 e ISO 27701:2019 – Gestão da Segurança da Informação e Gestão de Privacidade da Informação;

20.30.6.3. Certificação Data Protection Officer – DPO.

20.30.7. Prova que a empresa possui vínculo com os profissionais indicados por meio de da apresentação de contrato social, em se tratando de sócio da empresa; mediante cópia da Carteira de Trabalho e Previdência Social – CTPS, no caso de empregado; por meio de contrato de prestação de serviços; ou através de declaração de contratação futura do profissional;

20.30.8. No caso de apresentação de Declaração de Contratação futura do profissional, esta deve ser acompanhada de declaração de anuência do profissional, **devidamente assinada**.

20.31. Demais documentos e disposições serão elencados em Edital.

21. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

21.1. O valor estimado da contratação possui caráter sigiloso, conforme justificativa acostada ao ETP e não será tornado público antes de definido o resultado do julgamento das propostas.

22. ADEQUAÇÃO ORÇAMENTÁRIA

22.1. As despesas correrão por conta de dotação específica dos orçamentos de cada CONTRATANTE, sendo que no momento da contratação será especificada a dotação orçamentária;

22.2. O Ente CONTRATANTE quando da contratação especificará a classificação orçamentária.

Garibaldi, 18 de setembro de 2026.

RUDIMAR CABERLON:47751517034
Assinado de forma digital por RUDIMAR CABERLON:47751517034
Dados: 2026.09.18 08:53:10 -03'00'

RUDIMAR CABERLON
Diretor Executivo CISGA

Aprovo o presente Termo de Referência.

NELTON CARLOS CONTE:53096797072
Assinado de forma digital por NELTON CARLOS CONTE:53096797072
Dados: 2026.09.18 09:07:58 -03'00'

NELTON CARLOS CONTE
Presidente Consórcio Intermunicipal de Desenvolvimento Sustentável da Serra Gaúcha CISGA

ANEXO II
(EM FOLHA TIMBRADA DA EMPRESA)
PROPOSTA COMERCIAL *(modelo)*

PREGÃO ELETRÔNICO Nº 0011/2026 CP-CISGA – Registro de Preços

Apresentamos nossa proposta para aquisição do objeto da presente licitação, através do Pregão Eletrônico nº 0011/2026, acatando todas as estipulações consignadas no respectivo Edital e seus anexos.

1. IDENTIFICAÇÃO DA LICITANTE:

NOME DA EMPRESA:

CNPJ e INSCRIÇÃO ESTADUAL:

ENDEREÇO, TELEFONE e EMAIL:

RESPONSÁVEL PARA ASSINUTURA DA ATA e CARGO:

AGÊNCIA e Nº DA CONTA BANCÁRIA:

2. RELAÇÃO DOS BENS (READEQUADO AO LANCE VENCEDOR)

ITEM	**Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, compreendendo serviço de adequação à LGPD e manutenção recorrente, firewalls de próxima geração (NGFW), gerenciamento centralizado e retenção de logs, serviço gerenciado de monitoramento e resposta a incidentes (NOC/SOC/SIEM), software de antivírus com VPN/ZTNA, backup em nuvem, transceivers, treinamento e horas técnicas de suporte especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA.**	**UNIDADE**	**QUANTIDADE ESTIMADA**	**VALOR UNITÁRIO**	**VALOR TOTAL**

01	Implantação do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I, II, III.	UST (unidade)	20.208		
02	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I	Até 30.00 Habitantes (mês)	192		
03	Terceirização do Encarregado de Dados – Tipo I	Até 30.000 Habitantes (mês)	192		
04	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo II	De 30.001 até 50.000 habitantes (mês)	36		
05	Terceirização do Encarregado de Dados – Tipo II	De 30.001 até 50.000 habitantes (mês)	36		
06	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo III	De 50.001 até 100.000 habitantes (mês)	12		
07	Terceirização do Encarregado de Dados – Tipo III	De 50.001 até 100.000 habitantes (mês)	12		
08	Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente com	Endpoint (unidade)	68.928		

	setup/implantação e suporte de 12 meses.				
09	Operação Assistida e Treinamento para Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente.	UST (unidade)	7.680		
10	Solução de Detecção e Resposta a Incidentes em Endpoints (EDR) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928		
11	Operação Assistida e Treinamento para Solução de Detecção e Resposta a Incidentes em Endpoints (EDR)	UST (unidade)	7.680		
12	Solução de Proteção e Prevenção de Vazamento de Dados (DLP) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928		
13	Operação Assistida e Treinamento para Solução de Proteção e Prevenção de Vazamento de Dados (DLP).	Endpoint (unidade)	7.680		
14	Software de SIEM - Security Information&Event Managment com setup/implantação e suporte de 12 meses.	Ativo Monito-rado (unidade)	3.552		
15	Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra	Endpoint (unidade)	68.928		

	ataques cibernéticos, conformidade, maturidade com setup/implantação e suporte de 12 meses.				
16	Operação Assistida e Treinamento para Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos, conformidade, maturidade.	UST (unidade)	7.680		
17	Sistema de Backup Resilente, recuperação via DR Online com setup/implantação e suporte de 12 meses.	TB Protegido (unidade)	2.604		
18	Operação Assistida e Treinamento para Sistema de Backup Resilente, recuperação via DR Online.	UST (unidade)	7.680		
19	SOC - Security Operations Center – 8x5 com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	39.192		
20	SOC - Security Operations Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	33.288		
21	Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM), com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928		
22	Operação Assistida e Treinamento para Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM).	UST (unidade)	7.680		
23	Contratação de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados de ransomware com	Endpoint (unidade)	68.928		

	setup/implantação e suporte de 12 meses.				
24	Operação Assistida e Treinamento para Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados.	UST (unidade)	7.680		
25	Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928		
26	Operação Assistida e Treinamento para Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação.	UST (unidade)	7.680		
27	NOC – Network Operation Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	3.552		
28	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo I com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	5		
29	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo II com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	12		
30	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo III com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	6		
31	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo	Equipamento (unidade)	5		

	IV com setup/implantação e suporte de 12 meses.				
32	Subscrição anual de plataforma em nuvem de criptografia, anonimização e rastreabilidade documental.	Subscrição anual por munici-pio/Orgao (mês)	240		
33	Crédito de anonimização excedente à franquia	Mil páginas equivalentes (unidade)	303		
34	Crédito de custódia cifrada excedente à franquia	Mil arquivos (unidade)	125		
35	Crédito de armazenamento excedente à franquia	Gigabyte (unidade)	1.485		
36	Crédito de rastreabilidade excedente à franquia	Mil Páginas Marcadas (unidade)	157		
37	Operação Assistida e Treinamento para itens – 33 ao 36	UST (unidade)	7.680		
			VALOR TOTAL		

VALOR TOTAL DA PROPOSTA: R$ (XXX em números e por extenso)

DECLARO DE QUE MINHA PROPOSTA ECONÔMICA COMPREENDE A INTEGRALIDADE DOS CUSTOS para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

VALIDADE DA PROPOSTA COMERCIAL: no mínimo 60 (sessenta) dias contados a partir de sua data de entrega

[Cidade], [dia] de [mês] de [ano].

Nome do Representante Legal ou convencional da empresa
Função
CPF

ANEXO III
Minuta da ATA DE REGISTRO DE PREÇOS
N.º .....

[@DataContratoCompleta], O **[@NomeEntidade]**, entidade com personalidade jurídica de direito público, inscrita no CNPJ sob o nº [@CNPJEntidade], com sede na [@EnderecoEntidadeCompleto], [@CepEntidade], neste ato representado por sua [@CargoResponsavelEntidade], Sr. [@ResponsavelEntidade], eleito pela Assembleia Geral de 25 de novembro de 2025, doravante denominado **ORGÃO GERENCIADOR** e a empresa **[@NomeFornecedor]** pessoa jurídica de direito privado, situada na [@EnderecoFornecedor], [@CidadeUFCepFornecedor], inscrita no CNPJ sob o nº [@CNPJFornecedor], neste ato representada [@NomeEFuncaoRepresentantes], doravante denominada **FORNECEDORA**, firmam a presente Ata de Registro de Preços, regida pela Lei Federal nº 14.133, de 01 de abril de 2021, no Decreto n.º 11.462, de 31 de março de 2023, e pelos termos do edital, mediante as cláusulas e condições a seguir estabelecidas:

1 DO OBJETO

1.1 A presente Ata tem por objeto o registro de preços para a Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA, conforme especificações do Termo de Referência, que é parte integrante desta Ata, assim como as propostas cujos preços tenham sido registrados, independentemente de transcrição.

2 DOS PREÇOS, ESPECIFICAÇÕES E QUANTITATIVOS

2.1 O preço registrado, as especificações do objeto, as quantidades estimadas de cada item e as demais condições ofertadas na(s) proposta(s) seguem em anexo a esta ATA.
2.2.1 As Atas geradas do cadastro de reserva referente ao presente registro de preços constam no site oficial do CISGA, disponível em https://www.cisga.com.br/licitacoes.

3 ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

3.1 O órgão gerenciador será o Consórcio Intermunicipal de Desenvolvimento Sustentável da Serra Gaúcha – CP-CISGA.
3.2 São entes públicos participantes do registro de preços, os municípios de:

CISGA - RUA JACOB ELY, 498 – SALAS 4 E 5 – CENTRO, GARIBALDI – RS – CEP 95720-000.

ANDRÉ DA ROCHA - RUA MARCOLINO PEREIRA VIEIRA, Nº 1393, CENTRO, CEP: 95310-000 – CNPJ:90.483.066/0001-72.

ANTÔNIO PRADO - RUA FRANCISCO MARCANTÔNIO, Nº 57, CENTRO, CEP: 95250-000 - CNPJ: 87.842.233/0001-10.

CARLOS BARBOSA - RUA ASSIS BRASIL, Nº 11, CENTRO, CEP: 95185-000 - CNPJ: 88.587.183/0001-34.

FAGUNDES VARELA - AV. ALFREDO REALI, Nº300, CENTRO, CEP: 95333-000 - CNPJ: 91.566.893/0001-92.

FARROUPILHA - PRAÇA EMANCIPAÇÃO, 116, BAIRRO CENTRO, CEP 95170-444 - CNPJ: 89.848.949/0001-50.

FLORES DA CUNHA - RUA SÃO JOSÉ, 2500, CENTRO, CEP: 95270-000 - CNPJ: 87.843.819/0001-07.

GARIBALDI - RUA JÚLIO DE CASTILHOS, Nº 254, CENTRO, CEP:95720-000 - CNPJ: 88.594.999/0001-95.

MONTE BELO DO SUL - RUA SAGRADA FAMÍLIA, 533, CENTRO, CEP: 95718-000 - CNPJ: 91.987.669/0001-74.

NOVA ARAÇÁ - RUA ALEXANDRE GAZZONI, 200, CENTRO, CEP: 95350-000 - CNPJ: 87.502.902/0001-04.

NOVA BASSANO - RUA SILVA JARDIM, 505, CENTRO, CEP: 95340-000- CNPJ: 87.502.894/0001-04.

NOVA PRATA - AV. FERNANDO LUZATO, Nº 158, CENTRO, CEP: 95320-000 – CNPJ: 91.618.439/0001-38.

NOVA ROMA DO SUL - RUA JÚLIO DE CASTILHOS, Nº 895, CENTRO, CEP:95260-000 – CNPJ: 91.110.296/0001-59

PARAÍ - AVENIDA PRESIDENTE CASTELO BRANCO, 1033 - CENTRO, CEP: 95360-000 - CNPJ: 87.502.866/0001-50.

PINTO BANDEIRA - RUA SETE DE SETEMBRO, 689, CENTRO, CEP 95717-000 - CNPJ: 04.213.671/0001-91.

SANTA TEREZA - AVENIDA ITÁLIA, Nº 474, CENTRO, CEP: 95715-000 - CNPJ: 91.987.719/0001-13.

SÃO JORGE - AV. DALTRO FILHO, Nº 901, CENTRO, CEP 95365-000 - CNPJ: 91.566.851/0001-51.

SÃO MARCOS - AV. VENÂNCIO AIRES, Nº 720, CENTRO, CEP: 95190-000 - CNPJ: 88.818.299/0001-37.

VERANÓPOLIS – RUA ALFREDO CHAVES, Nº 366, CENTRO, CEP;95330-000 - CNPJ: 98.671.567/0001-09.

VILA FLORES - RUA FABIANO FERRETO, 200, CENTRO, CEP: 95334-000 - CNPJ: 91.566.869/0001-53.

3.2 Vedação a acréscimo de quantitativos

3.2.1 É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

4 DA ADESÃO À ATA DE REGISTRO DE PREÇOS

4.1 Desde que devidamente justificada a vantagem, a Ata de Registro de Preços decorrente deste certame poderá ser utilizada por órgãos e entidades da Administração Pública que não participaram dos procedimentos iniciais da licitação.

4.2 A utilização da Ata por órgãos não participantes fica condicionada à prévia consulta e aceitação do Órgão Gerenciador, bem como à concordância do fornecedor beneficiário do registro.

4.3. Nos termos do § 4º do art. 86 da Lei Federal nº 14.133, as aquisições ou contratações adicionais por órgãos não participantes não poderão exceder, por órgão ou entidade, a 50% (cinquenta por cento) dos quantitativos dos itens do edital e registrados na ata de registro de preços para o órgão gerenciador e órgãos participantes.

4.4 Nos termos do § 5º do art. 86 da Lei Federal nº 14.133, o quantitativo decorrente das adesões à ata de registro de preços não poderá exceder, na totalidade, ao dobro (200%) do quantitativo de cada item registrado para o órgão gerenciador e órgãos participantes, independentemente do número de órgãos não participantes que aderirem.

5 VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1 A validade da Ata de Registro de Preços será de 12 (doze) meses, contado a partir do primeiro dia útil subsequente à data de divulgação no PNCP, podendo ser prorrogada por igual período, mediante a anuência do fornecedor, desde que comprovado o preço vantajoso.

5.1.1 O contrato decorrente da Ata de Registro de preços terá sua vigência estabelecida no próprio instrumento contratual e observará no momento da contratação e a cada exercício financeiro a disponibilidade de créditos orçamentários, bem como a previsão no plano plurianual, quando ultrapassar 1 (um) exercício financeiro.

5.1.2 Na formalização do contrato ou do instrumento substituto deverá haver a indicação da disponibilidade dos créditos orçamentários respectivos.

5.2 A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de instrumento contratual, emissão de nota de empenho de despesa, autorização de compra ou outro instrumento hábil, conforme o art. 95 da Lei nº 14.133, de 2021.

5.2.1 O instrumento contratual de que trata o item 5.2 deverá ser assinado no prazo de validade da ata de registro de preços.

5.3 Os contratos decorrentes do sistema de registro de preços poderão ser alterados, observado o art. 124 da Lei nº 14.133, de 2021.

5.4 Após a homologação da licitação, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.4.1 Serão registrados na ata os preços e os quantitativos do adjudicatário, sendo vedada a possibilidade de o licitante oferecer na proposta quantitativo inferior ao máximo previsto no edital;

5.4.2 Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

5.4.2.1 Aceitarem cotar os bens com preços iguais aos do adjudicatário, observada a classificação da licitação;

5.4.2.3 Mantiverem sua proposta original.

5.5 Será respeitada, nas contratações, a ordem de classificação dos licitantes ou dos fornecedores registrados na ata.

5.6 O registro a que se refere o item 5.4.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.7 Para fins da ordem de classificação, os licitantes ou fornecedores que aceitarem reduzir suas propostas para o preço do adjudicatário antecederão aqueles que mantiverem sua proposta original.

5.8 A habilitação dos licitantes que comporão o cadastro de reserva somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

5.8.1 Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e

5.8.2 Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.9 O preço registrado com indicação dos licitantes e fornecedores será divulgado no PNCP e ficará disponibilizado durante a vigência da ata de registro de preços.

5.10 Após a homologação da licitação, o licitante mais bem classificado será convocado para assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital de licitação ou no aviso de contratação direta, sob pena de decair o direito, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021.

5.10.1 O prazo de convocação poderá ser prorrogado 1 (uma) vez, por igual período, mediante solicitação do licitante ou fornecedor convocado, desde que apresentada dentro do prazo, devidamente justificada, e que a justificativa seja aceita pela Administração.

5.10.2 A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.11 Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital ou no aviso de contratação, e observado o disposto no item 5.10, observando o item e subitens, fica facultado à Administração convocar os licitantes remanescentes do cadastro de reserva, na ordem de classificação, para fazê-lo em igual prazo e nas condições propostas pelo primeiro classificado.

5.12 Na hipótese de nenhum dos licitantes que compõem o cadastro de reserva, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

5.12.1 Convocar para negociação os demais licitantes ou fornecedores remanescentes cujos preços foram registrados sem redução, observada a ordem de classificação, com vistas à obtenção de preço melhor, mesmo que acima do preço do adjudicatário; ou

5.12.2 Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.

5.13 A existência de preços registrados implicará compromisso de fornecimento nas condições estabelecidas, mas não obrigará a Administração a contratar, facultada a realização de licitação específica para a aquisição pretendida, desde que devidamente justificada.

6 ALTERAÇÃO OU ATUALIZAÇÃO DOS PREÇOS REGISTRADOS

6.1 Os preços registrados poderão ser alterados ou atualizados em decorrência de eventual redução dos preços praticados no mercado ou de fato que eleve o custo dos bens, das obras ou dos serviços registrados, nas seguintes situações:

6.1.1 Em caso de força maior, caso fortuito ou fato do príncipe ou em decorrência de fatos imprevisíveis ou previsíveis de consequências incalculáveis, que inviabilizem a execução da ata tal como pactuada, nos termos da alínea "d" do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

6.1.2 Em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou a superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

6.1.3 Na hipótese de previsão no edital ou no aviso de contratação direta de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.2 **No caso do reajustamento**, o pedido de revisão (reequilíbrio econômico-financeiro) dos preços registrados será formulado, por escrito, pelo fornecedor signatário, dirigido ao órgão gerenciador por correio eletrônico endereçado ao e-mail contato2@cisga.com.br ou mediante protocolo no Sistema de Controle de Licitações e Contratos Administrativos STLICITA, se disponível, e conterá, sob pena de não conhecimento:

a) a indicação da ata, dos itens e dos preços registrados a que se refere;

b) o preço pretendido, acompanhado da respectiva memória de cálculo;

c) a descrição precisa do fato superveniente invocado, com a demonstração analítica do seu impacto sobre o custo do item e do nexo causal entre um e outro;

d) a documentação comprobatória pertinente, tal como: planilha de composição de custos que confronte as condições vigentes ao tempo da proposta e as atuais; notas fiscais de aquisição anteriores e posteriores ao fato; cotações e tabelas oficiais; os atos normativos correspondentes, na hipótese do subitem 6.1.2;

e) a declaração de que a variação alegada não constitui álea ordinária inerente ao risco do negócio.

6.3 O requerimento deverá ser formulado durante a vigência da ata e, na hipótese de prorrogação, antes da sua formalização, sob pena de preclusão (art. 131, parágrafo único, da Lei nº 14.133, de 2021, por identidade de razões).

6.4 **No trâmite**, a Administração terá o prazo de 1 (um) mês para decidir sobre o pedido de revisão, admitida a prorrogação motivada por igual período (art. 123, parágrafo único, da Lei nº 14.133, de 2021.

6.4.1. A contagem do prazo referido no item 6.3 somente se inicia com o recebimento da documentação comprobatória completa e consistente. Verificada a incompletude, o gerenciador intimará o requerente, uma única vez, para complementação no prazo de 5 (cinco) dias úteis, prorrogável mediante justificativa aceita; não suprida a falta, o pedido será arquivado, sem resolução de mérito;

6.4.2. A Administração não tem o dever de emitir decisão sobre requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do compromisso (art. 123, caput, da Lei nº 14.133, de 2021);

6.4.3. O pedido será instruído com manifestação técnica fundamentada do setor competente do gerenciador, facultada a requisição de subsídios aos órgãos participantes e à equipe técnica do certame, e, quando a formalização reclamar termo aditivo, com a análise jurídica cabível, a qual poderá ser referencial, a critério exclusivo do titular do Órgão de Assessoramento Jurídico, na esteira do teor expresso no art. 53, § 5º da Lei nº 14.133/2021;

6.4.4. A protocolização do pedido não autoriza a suspensão nem a redução do fornecimento: o fornecedor permanece vinculado às condições registradas até a decisão, sob pena de cancelamento do registro e das sanções cabíveis (itens 7.2.2 e 9.1 desta Ata; art. 156 da Lei nº 14.133, de 2021).

6.5 **Dos critérios de análise e decisão**. O deferimento somente será possível mediante o atendimento, de forma cumulativa, dos seguintes requisitos:

a) a comprovação da ocorrência de fato enquadrável no item 6.1 e do nexo causal com a variação do custo;

b) o caráter extraordinário da variação — flutuações ordinárias de preços, a inflação acumulada e as oscilações inerentes ao risco do negócio não autorizam a revisão;

c) a observância da repartição objetiva de riscos estabelecida nos instrumentos da contratação;

d) a limitação da recomposição ao estritamente necessário ao restabelecimento das condições efetivas da proposta (art. 37, XXI, da Constituição Federal), vedado o enriquecimento sem causa de qualquer das partes;

e) a observância do teto referencial do certame: o preço alterado ou atualizado não poderá, igualmente, exceder o valor máximo aceitável (valor de referência) adotado para o item nesta licitação, admitida a sua reapuração pelo gerenciador, contemporânea à decisão, mediante nova pesquisa de preços realizada na forma da IN SEGES/ME nº 65/2021 e segundo a metodologia da Planilha de Valores de Referência do certame, prevalecendo, em qualquer caso, o menor entre os limites das alíneas "d" e "e".

6.5.1. A alteração ou atualização deferida produzirá efeitos financeiros a contar da data do protocolo do requerimento completo, vedada a retroação a período anterior;

6.5.2. Se, comprovado o desequilíbrio decorrente dos estritos fatos autorizadores dos itens 6.1.1 e 6.1.2, a recomposição integral esbarrar nos limites das alíneas "d" e "e" do item 6.5, o pedido será deferido até o limite cabível, facultado ao fornecedor que demonstre a inviabilidade da manutenção do compromisso requerer a liberação do registro, sem aplicação de penalidade, na forma do art. 27 do Decreto nº 11.462/2023 e do item 7.2 desta Ata.

6.6 **Da formalização.** Deferido o pedido, por despacho motivado da autoridade competente:

6.6.1. a revisão fundada nos subitens 6.1.1 e 6.1.2 será formalizada por termo aditivo à ata (art. 124, II, "d", c/c art. 132 da Lei nº 14.133, de 2021); o reajustamento ou a repactuação, quando previstos (subitem 6.1.3), bem como as demais atualizações referidas no art. 136 da mesma Lei, serão registrados por simples apostilamento;

6.6.2. o instrumento será assinado por meio de assinatura digital qualificada ICP-Brasil, mediante acesso ao Sistema STLICITA, e divulgado no Portal Nacional de Contratações Públicas — PNCP;

6.6.3. o gerenciador comunicará a alteração ou atualização aos órgãos participantes e às entidades que tiverem firmado contratos decorrentes da ata, para os fins dos itens 7.1.4 e 7.2.6;

6.6.4. o indeferimento será comunicado ao requerente por decisão motivada, permanecendo íntegras as obrigações assumidas, na forma do subitem 6.3.4.

6.7 **Do reajustamento.** No caso do reajustamento, se previsto no edital, deverão ser respeitados a anualidade — contada da data do orçamento estimado da contratação (art. 25, §§ 7º e 8º, c/c art. 92, § 3º, da Lei nº 14.133, de 2021) — e o índice previsto, formalizando-se a variação por apostilamento.

6.8 **Da relação entre a ata e os contratos dela decorrentes.** A alteração ou atualização dos preços registrados não modifica, automaticamente, os contratos em curso: o reequilíbrio econômico-financeiro destes deverá ser postulado pelo contratado diretamente ao respectivo contratante e por este decidido, na forma dos arts. 124 a 136 da Lei nº 14.133, de 2021, e das cláusulas nona e décima quinta da minuta de contrato (Anexo IV do edital). Reciprocamente, o reequilíbrio eventualmente concedido em contrato não aproveita à ata nem a outros contratos.

6.8.1. Aplicam-se aos pedidos de reequilíbrio dos contratos decorrentes, no que couber, as regras de formalização, instrução, trâmite e critérios de decisão desta cláusula, competindo a decisão à autoridade competente do contratante.

6.8.2. O contratante que deferir reequilíbrio contratual comunicará a decisão ao gerenciador, para que este avalie a pertinência da instauração do procedimento previsto nesta cláusula e no item 7 quanto aos preços registrados.

7 NEGOCIAÇÃO DE PREÇOS REGISTRADOS

7.1 Na hipótese de o preço registrado tornar-se superior ao preço praticado no mercado por motivo superveniente, o órgão ou entidade gerenciadora convocará o fornecedor para negociar a redução do preço registrado.

7.1.1 Caso não aceite reduzir seu preço aos valores praticados pelo mercado, o fornecedor será liberado do compromisso assumido quanto ao item registrado, sem aplicação de penalidades administrativas.

7.1.2 Na hipótese prevista no item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam reduzir seus preços aos valores de mercado e não convocará os licitantes ou fornecedores que tiveram seu registro cancelado.

7.1.3 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, adotando as medidas cabíveis para obtenção de contratação mais vantajosa.

7.1.4 Na hipótese de redução do preço registrado, o gerenciador comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços para que avaliem a conveniência e a oportunidade de diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2 Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1 Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória ou a planilha de custos que demonstre a inviabilidade do preço registrado em relação às condições inicialmente pactuadas.

7.2.2 Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 10, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.3 Na hipótese de cancelamento do registro do fornecedor, nos termos do item anterior, o gerenciador convocará os fornecedores do cadastro de reserva, na ordem de classificação, para verificar se aceitam manter seus preços registrados, observado o disposto no item 5.8.

7.2.4 Se não obtiver êxito nas negociações, o órgão ou entidade gerenciadora procederá ao cancelamento da ata de registro de preços, nos termos do item 10, e adotará as medidas cabíveis para a obtenção da contratação mais vantajosa.

7.2.5 Na hipótese de comprovação da majoração do preço de mercado que inviabilize o preço registrado, conforme previsto no item 7.1 e no item 7.1.4, o órgão ou entidade gerenciadora atualizará o preço registrado, de acordo com a realidade dos valores praticados pelo mercado.

7.2.6 O órgão ou entidade gerenciadora comunicará aos órgãos e às entidades que tiverem firmado contratos decorrentes da ata de registro de preços sobre a efetiva alteração do preço

registrado, para que avaliem a necessidade de alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

8 REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

8.1 As quantidades previstas para os itens com preços registrados nas atas de registro de preços poderão ser remanejadas pelo órgão ou entidade gerenciadora entre os órgãos ou as entidades participantes do registro de preços.

8.2 O remanejamento somente poderá ser feito:

8.2 .1 De órgão ou entidade participante para órgão ou entidade participante;

8.3 O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

8.4 Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pela entidade participante, desde que haja prévia anuência da entidade que sofrer redução dos quantitativos informados.

9 CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

9.1 O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

9.1.1 Descumprir as condições da ata de registro de preços, sem motivo justificado;

9.1.2 Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;

9.1.3 Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou

9.1.4 Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

9.2 Na hipótese de aplicação de sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021, caso a penalidade aplicada ao fornecedor não ultrapasse o prazo de vigência da ata de registro de preços, poderá o órgão ou a entidade gerenciadora, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

9.3 O cancelamento de registros nas hipóteses previstas no item 9.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

9.4 Na hipótese de cancelamento do registro do fornecedor, o órgão ou a entidade gerenciadora poderá convocar os licitantes que compõem o cadastro de reserva, observada a ordem de classificação.

9.5 O cancelamento dos preços registrados poderá ser realizado pelo gerenciador, em determinada ata de registro de preços, total ou parcialmente, nas seguintes hipóteses, desde que devidamente comprovadas e justificadas:

9.5.1 Por razão de interesse público;

9.5.2 A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou

9.5.3 Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado se tornar superior ou inferior ao preço registrado, nos termos dos artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

10 DAS PENALIDADES

10.1 O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no edital

10.1.1 As sanções também se aplicam aos integrantes do cadastro de reserva no registro de preços que, convocados, não honrarem o compromisso assumido injustificadamente após terem assinado a ata.

10.2 É da competência do gerenciador a aplicação das penalidades decorrentes do descumprimento do pactuado nesta ata de registro de preço (art. 7º, inc. XIV, do Decreto nº 11.462, de 2023), exceto nas hipóteses em que o descumprimento disser respeito às contratações dos órgãos ou entidade participante, caso no qual caberá ao respectivo órgão participante a aplicação da penalidade (art. 8º, inc. IX, do Decreto nº 11.462, de 2023).

10.3 O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 9.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

11 CONDIÇÕES GERAIS

11.1 As condições gerais de execução do objeto, tais como os prazos e recebimento, as obrigações da Administração e do fornecedor registrado, penalidades e demais condições do ajuste, encontram-se definidos no Termo de Referência, ANEXO AO EDITAL.

11.2 Para firmeza e validade do pactuado, a presente Ata foi lavrada em .... (....) vias de igual teor, que, depois de lida e achada em ordem, vai assinada pelas partes e encaminhada cópia aos demais órgãos participantes (se houver).

Local e data

Assinaturas

Representante legal do órgão gerenciador e representante(s) legal(is) do(s) fornecedor(s) registrado(s) e testemunhas

ANEXO IV
MINUTA DE CONTRATO N°.....
PREGÃO ELETRÔNICO Nº 0011/2026 CP– CISGA

O CONSÓRCIO [...], pessoa jurídica de direito público interno, com sede administrativa na Rua [...], Nº [...], Bairro [...] inscrito no CNPJ sob nº [...], neste ato representado pelo Presidente Sr(a). ..... doravante denominado CONTRATANTE e, de outro lado a empresa [...], pessoa jurídica de direito privado, situada na [...], bairro [...] na cidade de [...], inscrita no CNPJ sob o nº [...], neste ato representado(a) por.....(nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, doravante denominada CONTRATADO, tendo em vista o que consta no Processo nº....., ajustam e contratam o fornecimento do objeto abaixo descrito, que se regerá pelo disposto neste Contrato, na Lei nº 14.133, de 1º de abril de 2021e suas alterações, no Decreto Federal nº 10.024/2019, de 20 de setembro de 2019, no Decreto Federal nº 11.462, de 31 de março de 2023 e na Resolução do Consórcio Intermunicipal de Desenvolvimento sustentável da Serra Gaúcha – CISGA nº 02, de 04 de maio de 2012, aplicando-se supletivamente as normas e princípios de direito público, de direito administrativo e de direito comum pertinentes.

CLÁUSULA PRIMEIRA – DO OBJETO
1.1 Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA, conforme especificações técnicas, requisitos e entregas definidos no Edital, Termo de Referência e Estudo Técnico Preliminar.

CLÁUSULA SEGUNDA – DO OBJETO E PREÇO
2.1 O valor total da contratação é de R$.....;
2.2 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.
2.3 O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA TERCEIRA – DO PAGAMENTO
3.1. O prazo para pagamento ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato. E esta condicionado ao aceite tecnico das entregas, a comprovação da regularidade fisal e ao cumprimento de marcos.
3.2. O cronograma de entregas observará, dentro do possível, metas de desenvolvimento e implantação da plataforma, de capacitação e materiais didáticos, monitoramento e suporte técnico contínuo e hospedagem e manutenção por 12 meses.

CLÁUSULA QUARTA – DO MODELO DE EXECUÇÃO DO OBJETO
4.1. A execução do objeto seguirá a seguinte dinâmica
4.1.1. A contratada deverá iniciar o desenvolvimento dos módulos no prazo máximo de **7 (sete) dias**, contados da assinatura do contrato, devendo disponibilizar a Plataforma Virtual plenamente operacional no prazo de até **90 (noventa) dias**, também contados da assinatura do instrumento contratual.
4.1.2. Todo o processo de desenvolvimento e implantação da solução será acompanhado e supervisionado pela Contratante.

4.2 Suporte e Manutenção
4.2.1. A CONTRATADA deverá manter o serviço de suporte técnico para todos os

itens deste Termo de Referência disponível 8 (oito) horas por dia, 5 (cinco) dias por semana, exceto nos períodos destinados a manutenção programada;

4.2.2. A severidade do problema/incidente será informada pela CONTRANTE, de acordo com os critérios da ocorrência, conforme classificação descritos na tabela de suporte técnico definida abaixo;

4.2.3. De acordo com a classificação da severidade, a CONTRATADA deverá cumprir os prazos conforme classificação descrita na tabela de SLA abaixo;

4.2.4. Entende-se por Retorno à Operação o tempo decorrido entre o início do chamado técnico e o encaminhamento da solução;

4.2.5. Deverá ser disponibilizado um canal de comunicação para contato de suporte técnico para o caso de bug/problemas técnicos, bem como indisponibilidade do ambiente ou questões referentes à taxa de atualização;

4.2.6. A abertura de chamados poderá ser feita pelos administradores do sistema da CONTRANTE, ou diretamente pelos usuários. Se o chamado encaminhado não estiver relacionado a dúvidas na operação do serviço, eles deverão orientar o solicitante a encaminhar a demanda ao suporte operacional;

4.2.7. Um chamado técnico somente poderá ser considerado encerrado após confirmação do responsável indicado pela CONTRANTE, e o término do atendimento se dará com a disponibilidade do serviço para uso em perfeitas condições de funcionamento no local onde estiver instalado;

4.2.8. Caso o chamado não se refira ao objeto deste termo de referência, ou ainda, por falta de elementos essenciais ao seu entendimento, a CONTRATADA deverá comunicar formalmente a CONTRANTE, acerca do encerramento do chamado, apresentando a respectiva justificativa, ou solicitar informações complementares para resolução do chamado;

4.2.9. Atualização A CONTRATADA deverá manter a(s) soluçao(oes) atualizada(s) e compatível(eis) com as novas versões e atualizações dos sistemas operacionais, componentes e navegadores que forem lançados durante a vigência do contrato;

4.2.10. A CONTRATADA deverá prestar os serviços de suporte e manutenção contínuos, durante a vigência do contrato, da(s) soluçao(oes). Este serviço visa garantir o funcionamento ininterrupto da(s) soluçao(oes) e a atualização constante de suas funcionalidades e a pronta assistência para quaisquer questões técnicas ou operacionais que possam surgir, deverão atender aos seguintes requisitos:

- Atendimento a Incidentes: Suporte ágil para resolução de problemas técnicos, erros ou falhas na plataforma, com tempos de resposta definidos em SLA (Service Level Agreement);
- Dúvidas e Orientações de Uso: Esclarecimento de dúvidas sobre as funcionalidades da plataforma, auxílio na interpretação de relatórios e orientações para o uso otimizado dos recursos;
- Canais de Comunicação: Disponibilidade de canal de suporte via telefone ou e-mail para facilitar a comunicação e agilizar o atendimento;
- Atualizações de Software: Garantia de que a plataforma esteja sempre com as versões mais recentes, incluindo correções de bugs, melhorias de desempenho e novas funcionalidades;
- Ajustes e Otimizações: Realização de ajustes e otimizações na configuração da plataforma para assegurar que ela opere com máxima eficiência e performance, adaptando-se às necessidades da sua infraestrutura;
- Gestão de Integrações: Manutenção das integrações com outras ferramentas de segurança da informação, garantindo que o fluxo de dados e informações seja contínuo e sem interrupções;

- Melhoria Contínua: A plataforma deve evoluir para incorporar novas tecnologias e atender às futuras demandas do mercado de segurança da informação;
- Verificação de Saúde: Monitoramento proativo da saúde e integridade dos componentes da plataforma, identificando potenciais gargalos ou falhas antes que impactem a operação;
- Otimização de Banco de Dados: Manutenção e otimização do banco de dados da plataforma para garantir a agilidade na recuperação e análise das informações de risco e conformidade.

4.2.11. O processo ocorrerá da seguinte forma:

- Prévia análise das necessidades pela CONTRANTE e CONTRATADA;
- Caso seja um desenvolvimento já previsto no Termo de Referência, a manutenção não deverá incorrer em ônus à CONTRATANTE;
- Quaisquer alterações e ou manutenções, bem como, o pagamento pelos serviços prestados (quando houver), estarão condicionados à homologação por parte da Contratante bem como ao fornecimento de documentação atualizada técnica e funcional.

CLÁUSULA QUINTA – DAS OBRIGAÇÕES PERTINENTES À LGPD

5.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD) alterada pela Lei nº 13.853, de 2019, 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;

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

5.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei;

5.4. Terminado o tratamento dos dados nos termos do art. 15 da LGPD, é dever do contratado 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;

5.5. A CONTRATADA obriga-se a garantir a confidencialidade dos dados coletados da CONTRATANTE por meio de uma política interna de privacidade, a fim de respeitar, por si, seus funcionários e seus prepostos, o objetivo do presente termo;

5.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD;

5.7. Conforme prevê a Lei Geral de Proteção de Dados, obriga-se a CONTRATADA a executar os seus trabalhos e tratar os dados da CONTRATANTE respeitando os princípios da finalidade, adequação, transparência, livre acesso, segurança, prevenção e não discriminação;

5.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados;

5.9. Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto à eventual descarte realizado;

5.10. 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;

5.11. A contratada deverá manter backups, adotar criptografia e comunicar eventuais incidentes.
5.12. O contrato está sujeito a ser alterado nos procedimentos pertinentes ao tratamento de dados pessoais, quando indicado pela autoridade competente, em especial a ANPD por meio de opiniões técnicas ou recomendações, editadas na forma da LGPD.

CLÁUSULA SEXTA – DOS PAPÉIS E RESPONSABILIDADES

6.1. São obrigações da CONTRATANTE:

a) receber, fiscalizar, orientar, contestar, dirimir dúvidas emergentes da execução do objeto contratado;
b) nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução dos contratos;
c) encaminhar formalmente a demanda por meio de Ordem de Serviço ou Autorização de Fornecimento, de acordo com os critérios estabelecidos no Termo de Referência;
d) receber o serviço prestado pelo contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
e) notificar a contrata, por escrito, sobre vícios, defeitos ou incorreções verificadas no objeto fornecido, para que seja por ele reparado ou corrigido, no total ou em parte, às suas expensas;
f) aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, quando aplicável;
g) liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
h) comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução;
i) resguardar os direitos de propriedade intelectual e direitos autorais da solução sobre os diversos artefatos e produtos cuja criação ou alteração seja objeto da relação contratual pertençam à Administração, incluindo a documentação, o código-fonte de aplicações, os modelos de dados e as bases de dados, justificando os casos em que isso não ocorrer;
j) fornecer à Contratada todas as informações, os esclarecimentos, os documentos e as demais condições necessárias à execução do contrato;
k) zelar para que sejam cumpridas as obrigações assumidas pela licitante vencedora e para que sejam mantidas todas as condições de habitação e qualificação exigidas na licitação.

6.2. São obrigações do CONTRATADA:

a) indicar formalmente preposto apto a representá-la junto à contratante, que deverá responder pela fiel execução do contrato;
b) assumir a responsabilidade pela prestação dos serviços descritos neste Termo de Referência, no Edital e no Contrato, inclusive fornecer o serviço licitado tomando especial cuidado para que os módulos sejam aqueles atendam as especificações técnicas constante neste Termo;
c) dar fiel execução integral ao objeto desta contratação, bem como providenciar às suas expensas e a contento do Contratante todas as substituições e correções que se fizerem necessárias;
d) atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;
e) reparar quaisquer danos diretamente causados à contratante ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos serviços pela contratante;
f) propiciar todos os meios necessários à fiscalização do contrato pela contratante, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;
g) manter, durante toda a execução do contrato, as mesmas condições da habilitação;
h) quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução;

i) não transferir a terceiros, por qualquer forma, nem mesmo parcialmente, as obrigações assumidas, nem subcontratar qualquer das prestações a que está obrigada, sem prévia anuência da contratante;
j) deverá garantir que a plataforma virtual, após implementação e pleno funcionamento, estará sujeito a ajustes e alterações para atendimento de situações especificas requeridas pelo Consórcio Público, mediante requerimento e orçamento prévio, desde que tais alterações não interfiram na estrutura básica e demais funcionalidades do sistema;
k) dar ciência imediata e por escrito à Contratante sobre qualquer anormalidade verificada na execução dos serviços;
l) garantir que os serviços de assistência técnica, suporte, deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;
m) ceder os direitos de propriedade intelectual e direitos autorais da solução sobre os diversos artefatos e produtos produzidos em decorrência da relação contratual, incluindo a documentação, os modelos de dados e as bases de dados à Administração;
n) manter ciente que os dados existentes no sistema de gestão pública são de propriedade da contratante e o armazenamento desses dados deve estar em perfeita conformidade com os ditames da Lei Federal nº 13.709, de 14 de agosto de 2018, também conhecida por Lei Geral de Proteção de Dados Pessoais (LGPD).

CLÁUSULA SÉTIMA – DO DESENVOLVIMENTO E IMPLEMENTAÇÃO

7.1. A contratada deverá iniciar o desenvolvimento dos módulos no prazo máximo de **7 (sete) dias**, contados da assinatura do contrato, devendo disponibilizar a Plataforma Virtual plenamente operacional no prazo de até **90 (noventa) dias**, também contados da assinatura do instrumento contratual.
7.2. Todo o processo de desenvolvimento e implantação da solução será acompanhado e supervisionado pela Contratante.

CLÁUSULA OITAVA – DA DOTAÇÃO ORÇAMENTÁRIA

8.1. As despesas decorrentes da contração, objeto do presente contrato, correrão a conta de dotação específica, e terá a seguinte classificação orçamentária:
Unidade:
Função:
Subfunção:
Programa:
Proj/Ativ.:
Recurso:
Dotação Principal:

CLÁUSULA NONA – DAS INFRAÇÕES E SANÇÕES ADMINISTRATIVAS

9.1. Comete infração administrativa, nos termos da Lei nº 14.133, de 2021, o contratado 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.
9.2. Serão aplicadas ao contratado que incorrer nas infrações acima descritas as seguintes sanções:
i. Advertência, quando o contratado der causa à inexecução parcial do contrato, sempre que não

se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);

ii. 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 (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. 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 (art. 156, §5º, da Lei nº 14.133, de 2021).

iv. Multa:

1. Moratória de 0,5% (meio por cento) por dia de atraso injustificado sobre o valor da parcela inadimplida, até o limite de 30 (trinta) dias;

i. O atraso superior a 30 dias será considerado inexecução total do contrato e autoriza a Administração a promover a extinção do contrato por descumprimento ou cumprimento irregular de suas cláusulas, conforme dispõe o inciso I do art. 137 da Lei n. 14.133, de 2021.

2. Compensatória, para as infrações descritas nas alíneas "e" a "h" do subitem 9.1, de 30 % (trinta por cento) do valor do Contrato.

3. Compensatória, para a inexecução total do contrato prevista na alínea "c" do subitem 9.1, de 20% (vinte por cento) a 30% (trinta por cento) do valor do Contrato.

4. Para infração descrita na alínea "b" do subitem 9.1, a multa será de 15% (quinze por cento) a 20% (vinte por cento) do valor do Contrato.

5. Para infrações descritas na alínea "d" do subitem 9.1, a multa será de 10% (dez por cento) a 20% (vinte por cento) do valor do Contrato.

6. Para a infração descrita na alínea "a" do subitem 9.1, a multa será de 5% (cinco por cento) a 10% (dez por cento) do valor do Contrato.

9.3. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado ao Contratante (art. 156, §9º, da Lei nº 14.133, de 2021)

9.4. Todas as sanções previstas no Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

9.5. Antes da aplicação da multa será facultada a defesa do interessado no prazo de 15 (quinze) dias úteis, contado da data de sua intimação (art. 157, da Lei nº 14.133, de 2021)

9.6. Se a multa aplicada e as indenizações cabíveis forem superiores ao valor do pagamento eventualmente devido pelo Contratante ao Contratado, além da perda desse valor, a diferença será descontada da garantia prestada ou será cobrada judicialmente (art. 156, §8º, da Lei nº 14.133, de 2021).

9.7. Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 15 (quinze) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

9.8. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado em qualquer caso, observando-se o procedimento previsto no caput e parágrafos do art. 158 da Lei nº 14.133, de 2021, para as penalidades de impedimento de licitar e contratar e de declaração de inidoneidade para licitar ou contratar.

9.9. Na aplicação das sanções serão considerados (art. 156, §1º, da Lei nº 14.133, de 2021):

a) a natureza e a gravidade da infração cometida;

b) as peculiaridades do caso concreto;

c) as circunstâncias agravantes ou atenuantes;

d) os danos que dela provierem para o Contratante;

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

9.10. Os atos previstos como infrações administrativas na Lei nº 14.133, de 2021, ou em outras leis de licitações e contratos da Administração Pública que também sejam tipificados como atos lesivos na Lei nº 12.846, de 2013, serão apurados e julgados conjuntamente, nos mesmos autos, observados o rito procedimental e autoridade competente definidos na referida Lei (art. 159).

9.11. A personalidade jurídica do Contratado poderá ser desconsiderada sempre que utilizada com abuso do direito para facilitar, encobrir ou dissimular a prática dos atos ilícitos previstos neste Contrato

ou para provocar confusão patrimonial, e, nesse caso, todos os efeitos das sanções aplicadas à pessoa jurídica serão estendidos aos seus administradores e sócios com poderes de administração, à pessoa jurídica sucessora ou à empresa do mesmo ramo com relação de coligação ou controle, de fato ou de direito, com o Contratado, observados, em todos os casos, o contraditório, a ampla defesa e a obrigatoriedade de análise jurídica prévia (art. 160, da Lei nº 14.133, de 2021).

9.12. O Contratante deverá, no prazo máximo de 15 (quinze) dias úteis, contado da data de aplicação da sanção, informar e manter atualizados os dados relativos às sanções por ela aplicadas, para fins de publicidade no Cadastro Nacional de Empresas Inidôneas e Suspensas (Ceis) e no Cadastro Nacional de Empresas Punidas (Cnep), instituídos no âmbito do Poder Executivo Federal. (Art. 161, da Lei nº 14.133, de 2021).

9.13. As sanções de impedimento de licitar e contratar e declaração de inidoneidade para licitar ou contratar são passíveis de reabilitação na forma do art. 163 da Lei nº 14.133/21.

9.14. Os débitos do contratado para com a Administração contratante, resultantes de multa administrativa e/ou indenizações, não inscritos em dívida ativa, poderão ser compensados, total ou parcialmente, com os créditos devidos pelo referido órgão decorrentes deste mesmo contrato ou de outros contratos administrativos que o contratado possua com o mesmo órgão ora contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

CLÁUSULA DÉCIMA– DA VIGÊNCIA

10.1. O prazo de vigência da contratação é de 12 (doze) meses, contados a partir do primeiro dia útil subsequente à data de divulgação no PNCP, na forma do artigo 105 da Lei n° 14.133, de 2021.

10.1.1. O prazo de vigência será automaticamente prorrogado, independentemente de termo aditivo, quando o objeto não for concluído no período firmado acima, ressalvadas as providências cabíveis no caso de culpa do contratado, previstas neste instrumento.

10.1.2. Tratando-se de contratação que prevê operação continuada do sistema, prazo de vigência da contratação é de 12 (doze) meses, prorrogável para até 10 anos (máximo de 10 anos, incluindo prorrogações), contados do(a) a partir do primeiro dia útil subsequente à data de divulgação no PNCP na forma do artigo 107 da Lei n° 14.133, de 2021.

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

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

CLÁUSULA DÉCIMA PRIMEIRA – DO REAJUSTE

11.1. Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, contado da data limite para a apresentação das propostas.

11.2. Após o interregno de um ano, e independentemente de pedido da CONTRATADA, os preços iniciais serão reajustados, mediante a aplicação, pela CONTRATANTE, do Indice de Custo da Tecnologia da Informação (ICTI), exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade, com base na seguinte fórmula:

$V_R = V_O \text{ X } \left(\frac{If}{Il}\right)$, onde =

V_R = **Valor reajustado** (novo preço do contrato);

V_O = **Valor original** do contrato ou parcela a ser reajustada;

I_F = **Índice final**, correspondente ao número-índice do mês de corte do reajuste;

I_I = **Índice inicial**, correspondente ao número-índice da data-base (ex: data do orçamento estimado).

11.3. Caso o índice de reajuste (ICTI) apresente variação negativa ou zero, o valor do contrato será mantido inalterado até o próximo período de reajuste.

- O contratante será notificado do valor atualizado por escrito, com antecedência mínima de 15 (quinze) dias antes da data do reajuste.

11.4. Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
11.5. No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).
11.6. Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
11.7. Caso o(s) índice(s) estabelecido(s) para reajustamento venha(m) a ser extinto(s) ou de qualquer forma não possa(m) mais ser utilizado(s), será(ão) adotado(s), em substituição, o(s) que vier(em) a ser determinado(s) pela legislação então em vigor.
11.8. Na ausência de previsão legal quanto ao índice substituto, as partes elegerão novo índice oficial, para reajustamento do preço do valor remanescente, por meio de termo aditivo.
11.9. O reajuste será realizado por apostilamento.

CLÁUSULA DÉCIMA SEGUNDA – DOS MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS
12.1. 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 serviço constam no Termo de Referência, anexo a este Contrato.
12.2. A execução será acompanhada por fiscal designado, que poderá solicitar ajustes, rejeitar entregas, determinar correçoes ou aplicar sanções.

CLÁUSULA DÉCIMA TERCEIRA – DOS MECANISMOS FORMAIS DE COMUNICAÇÃO
13.1. São definidos como mecanismos formais de comunicação, entre a Contratante e o Contratado, os seguintes:
13.1.1. Ordem de Serviço/Autorização de Fornecimento;
13.1.2. Ata de Reunião;
13.1.3. Ofício;
13.1.4. Sistema de abertura de chamados;
13.1.5. E-mails e Cartas;
13.1.6. Entre outros meios.

CLÁUSULA DÉCIMA QUARTA – DA SUBCONTRATAÇÃO
14.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA DÉCIMA QUINTA – DA GARANTIA DE EXECUÇÃO
15.1. Não haverá exigência de garantia contratual da execução, consoante fundamentado no Estudo Técnico Preliminar.

CLÁUSULA DÉCIMA SEXTA – DA RESCISÃO OU EXTINÇÃO CONTRATUAL
16.1. São causas que podem provocar a rescisão contratual: o descumprimento contratual, a falência, a paralisação, a irregularidade fiscal e o interesse público;
16.2. O contrato será extinto quando cumpridas as obrigações de ambas as partes, ainda que isso ocorra antes do prazo estipulado para tanto.
16.3. 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.
16.3.1. Quando a não conclusão do contrato referida no item anterior decorrer de culpa do contratado:
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 SÉTIMA – DOS CASOS OMISSOS

17.1. 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 OITAVA – DAS ALTERAÇÕES

18.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021 e somente são permitidas dentro dos limites legais e mediante termo aditivo;

18.2. O contratado é obrigado 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.

18.3. As alterações contratuais deverão ser promovidas mediante celebração de termo aditivo, submetido à prévia aprovação da consultoria 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).

18.4. 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.

18.5. As alterações que digam respeito à excepcional e imprevisível substituição do fabricante e/ou modelo do veículo contemplado(s) neste contrato obedecerão, naquilo que pertinentes, à disciplina estatuída no item 6 do Termo de Referência, o qual minudencia a sistemática atinente ao pedido e ao trâmite, considerando-se aqui transcrito, em sua integralidade.

CLÁUSULA DÉCIMA NOVA – DA PUBLICAÇÃO

19.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei n.º 14.133, de 2021, e ao art. 8º, §2º, da Lei n. 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n. 7.724, de 2012.

CLÁUSULA VIGÉSIMA – DO FORO

20.1 É competente o foro da Comarca de (Município Sede do Contratante) / RS___ para dirimir quaisquer dúvidas, porventura, oriundas do presente Contrato.

E por estarem justas e compromissadas, as partes assinam o presente contrato de fornecimento em [nº de vias] vias de igual teor e forma.

..... (UF), ... de ..... de.....
Presidente Consórcio Intermunicipal de Desenvolvimento
Sustentável da Serra Gaúcha CISGA

Fornecedor

Testemunhas: Assessoria Jurídica

ANEXO V
(EM FOLHA TIMBRADA DA PESSOA JURÍDICA)
DECLARAÇÃO - Habilitação (Conjunta)
(MODELO)

[Razão Social], CNPJ sob o nº [nº CNPJ], sediada à [nome rua/avenida, nº, complemento, bairro, Cidade /UF], DECLARA, sob as penas da lei, que:

a) Atende aos requisitos de habilitação e responderá pela veracidade das informações prestadas, na forma da lei, conforme art. 63, I da lei 14.133/2021;

b) Não foi declarada inidônea por Ato da Administração Pública;

c) Não emprega menor de 18 (dezoito) anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 (dezesseis) anos em qualquer trabalho, salvo na condição de aprendiz, a partir de quatorze anos, nos termos do inciso XXXIII, do art. 7º da CF/1988, nos termos do inciso VI do art. 68 da Lei nº 14.133/21;

d) Não possui, em toda sua cadeia produtiva, empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

e) Cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social, previstas em lei e em outras normas específicas, conforme art. 63, IV da lei 14.133/2021;

f) Não mantém vínculo, nem seus empregados, de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, e que nenhum de seus empregados deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, consoante art. 14, IV da Lei nº 14.133/21;

[Cidade], [dia] de [mês] de [ano].

Nome do Representante legal ou convencional da empresa
Função
RG e CPF

ANEXO VI
(EM FOLHA TIMBRADA DA PESSOA JURÍDICA)
DECLARAÇÃO EXCLUSIVA ME/EPP
(MODELO)

[Razão Social], CNPJ sob o nº [nº CNPJ], sediada à [nome rua/avenida, nº, complemento, bairro, Cidade /UF], DECLARA, sob as penas da lei, que:

Cumpre os requisitos estabelecidos no artigo 3°da Lei Complementar nº 123, de 2006, estando apta a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos § 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021, sendo, portanto, observado o limite de R$ 4.800.000,00 na licitação e, ainda, que no ano-calendário de realização da licitação, não foram celebrados contratos com a Administração Pública, cujos valores somados extrapolem a receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

[Cidade], [dia] de [mês] de [ano].

Nome do Representante legal ou convencional da empresa
Função
RG e CPF

ANEXO VII
(EM FOLHA TIMBRADA DA PESSOA JURÍDICA)
DECLARAÇÃO EXCLUSIVA COOPERATIVA
(MODELO)

[Razão Social], CNPJ sob o nº [nº CNPJ], sediada à [nome rua/avenida, nº, complemento, bairro, Cidade /UF], DECLARA, sob as penas da lei, que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021, para participar da licitação, sendo que:

a) a constituição e o funcionamento da cooperativa observam as regras estabelecidas na legislação aplicável, em especial a Lei nº 5.764, de 16 de dezembro de 1971, a Lei nº 12.690, de 19 de julho de 2012, e a Lei Complementar nº 130, de 17 de abril de 2009;

b) apresenta demonstrativo de atuação em regime cooperado, com repartição de receitas e despesas entre os cooperados;

c) qualquer cooperado, com igual qualificação, é capaz de executar o objeto contratado, vedado à Administração indicar nominalmente pessoas;

d) o objeto da licitação refere-se, em se tratando de cooperativas enquadradas na Lei nº 12.690, de 19 de julho de 2012, a serviços especializados constantes do objeto social da cooperativa, a serem executados de forma complementar à sua atuação.

[Cidade], [dia] de [mês] de [ano].

Nome do Representante legal ou convencional da empresa
Função
RG e CPF

ANEXO VIII
(EM FOLHA TIMBRADA DA PESSOA JURÍDICA)
PREGÃO ELETRÔNICO Nº 0011/2026 – CISGA

DECLARAÇÃO E LISTAGEM DE IDENTIFICAÇÃO DOS PROFISSIONAIS ENVOLVIDOS NA PRESTAÇÃO DE SERVIÇOS

Eu, _____ (Nome representante Legal da Pessoa Jurídica), representando _____ (nome da pessoa jurídica), inscrito(a) sob o CNPJ n° _____(número do CNPJ), DECLARO para fins relacionados ao Pregão Eletrônico n° 0011/2026 - CISGA, na forma da Lei Federal n° 14.133/21, que os profissionais envolvidos e/ ou atuantes na prestação dos serviços para os quais a pessoa jurídica pleiteia constam da listagem abaixo:

NOME DO PROFISSIONAL	CARGO /FUNÇÃO	ÁREA DE ATUAÇÃO	TIPO DE VÍNCULO

_____, em _____ de _____ de 20__.

_____
(assinatura e identificação do responsável legal/procurador da licitante)
Cargo
Nome:
RG:

ANEXO IX
CATÁLOGO TÉCNICO DE UNIDADE DE SERVIÇO TÉCNICO (UST)

1. OBJETIVO

1.1. O presente Anexo tem por objetivo estabelecer o Catálogo Técnico de Unidade de Serviço Técnico (UST), definindo critérios objetivos para mensuração, execução, aceite e faturamento dos serviços especializados relacionados à operação assistida, implantação, sustentação, treinamento, consultoria técnica, monitoramento, resposta a incidentes, hardening, integração, parametrização e demais serviços técnicos especializados previstos neste Termo de Referência.
1.2. A adoção do modelo de UST visa garantir:

- padronização da mensuração dos serviços;
- previsibilidade contratual;
- rastreabilidade operacional;
- transparência na execução;
- proporcionalidade entre esforço técnico e remuneração;
- auditabilidade das entregas;
- compatibilidade com ambientes de tecnologia da informação e segurança cibernética.

2. DEFINIÇÃO DE UST

2.1. Para fins deste Termo de Referência, considera-se Unidade de Serviço Técnico (UST) a unidade abstrata de mensuração utilizada para quantificar serviços técnicos especializados de tecnologia da informação, segurança da informação, proteção de dados pessoais e cibersegurança, considerando:

- complexidade técnica;
- criticidade;
- especialização profissional requerida;
- esforço operacional;
- impacto no ambiente;
- tempo médio estimado de execução;
- risco associado à atividade.

2.2. A UST não se confunde com hora técnica ou posto de trabalho.

3. REGRAS GERAIS DE MENSURAÇÃO

3.1. Os serviços serão medidos exclusivamente mediante:

- ordem de serviço;

- chamado técnico;
- plano de atividade;
- execução validada;
- aceite formal da CONTRATANTE.

3.2. A simples disponibilização de profissionais não gera direito automático à medição ou faturamento de UST.

3.3. Somente serão consideradas passíveis de medição as atividades efetivamente executadas e comprovadas.

3.4. Cada atividade poderá possuir:

- UST fixa;
- UST variável;
- UST mínima;
- fator multiplicador de complexidade.

3.5. As atividades executadas deverão possuir rastreabilidade mínima contendo:

- identificação da atividade;
- técnico responsável;
- data e horário;
- ativo ou sistema relacionado;
- evidências técnicas;
- resultado obtido;
- classificação de criticidade;
- tempo de execução;
- aceite do fiscal técnico.

4. CLASSIFICAÇÃO DE COMPLEXIDADE
4.1. BAIXA COMPLEXIDADE

4.1.1. Atividades operacionais padronizadas, repetitivas ou de baixo impacto. **Exemplos:**

- onboarding simples;
- ajuste de política;
- criação de usuário;

- configuração básica;
- geração de relatório;
- atualização simples;
- suporte operacional.

Fator de complexidade: 1,0

4.2. MÉDIA COMPLEXIDADE

4.2.1. Atividades que demandem análise técnica, integração moderada ou conhecimento especializado.
Exemplos:

- tuning;
- criação de regras;
- integração;
- investigação inicial;
- análise de eventos;
- parametrização avançada;
- revisão de políticas.

Fator de complexidade: 1,5

4.3. ALTA COMPLEXIDADE

4.3.1. Atividades críticas, estratégicas, emergenciais ou que envolvam elevado risco operacional ou de segurança. **Exemplos:**

- resposta a incidente;
- contenção de ransomware;
- análise forense;
- hardening avançado;
- recuperação de desastre;
- investigação avançada;
- integração crítica;
- arquitetura Zero Trust;
- remediação crítica.

4.3.2. Fator de complexidade: 2,0

5. CATÁLOGO TÉCNICO DE SERVIÇOS E UST

ITEM	SERVIÇO	COMPLEXIDADE	UST
1	Implantação inicial de solução	Alta	40
2	Onboarding de endpoint	Baixa	0,2
3	Onboarding de servidor	Média	1
4	Integração de ferramenta via API	Alta	12
5	Configuração de política de segurança	Média	2
6	Criação de regra SIEM	Média	3
7	Ajuste de correlação SIEM	Média	2
8	Criação de dashboard	Média	4
9	Parametrização DLP	Média	3
10	Ajuste de política DLP	Média	2
11	Investigação de incidente baixa criticidade	Média	4
12	Investigação de incidente alta criticidade	Alta	12
13	Contenção de incidente	Alta	8
14	Resposta a ransomware	Alta	30
15	Execução de playbook	Média	2
16	Criação de playbook	Média	6
17	Hardening de endpoint	Média	2
18	Hardening de servidor	Alta	12
19	Revisão de vulnerabilidade	Média	3
20	Varredura de vulnerabilidades	Média	4
21	Remediação de vulnerabilidade crítica	Alta	10
22	Configuração de backup	Média	4
23	Teste de restore	Média	6
24	Execução de DR Test	Alta	20
25	Configuração de microsegmentação	Alta	15
26	Configuração Zero Trust	Alta	20
27	Integração RMM	Média	4
28	Atualização de agente	Baixa	0,1
29	Ajuste de políticas antiransomware	Média	3
30	Revisão de arquitetura de segurança	Alta	16
31	Reunião técnica operacional	Baixa	1
32	Workshop técnico	Média	6
33	Treinamento operacional até 4h	Média	8
34	Treinamento avançado até 8h	Alta	16
35	Criação de relatório executivo	Média	3
36	Criação de relatório técnico detalhado	Média	5
37	Apoio em auditoria	Alta	12
38	Apoio em incidente LGPD	Alta	15
39	Elaboração de RIPD	Alta	20
40	Revisão de política de segurança	Média	6
41	Revisão de política de privacidade	Média	6
42	Apoio em atendimento ANPD	Alta	20
43	Análise de conformidade de fornecedor	Média	5

44	Assessment de maturidade	Alta	20
45	Revisão de controles CIS/NIST	Alta	12
46	Criação de baseline de segurança	Alta	10
47	Suporte técnico remoto	Baixa	1
48	Atendimento emergencial crítico	Alta	15
49	Integração com SIEM externo	Alta	10
50	Criação de automação SOAR	Alta	15

6. FATORES MULTIPLICADORES

6.1. Poderão ser aplicados fatores multiplicadores de complexidade nas seguintes hipóteses:

SITUAÇÃO	FATOR
Execução fora do horário comercial	1,5
Execução em ambiente crítico	1,5
Incidente de segurança ativo	2,0
Atuação emergencial	2,0
Ambiente com mais de 1.000 ativos	1,5
Atuação presencial	1,3

7. SERVIÇOS NÃO PREVISTOS

7.1. Serviços não previstos expressamente neste catálogo poderão ser executados mediante:

- justificativa técnica;
- definição prévia de equivalência de UST;
- autorização formal da CONTRATANTE.

8. CRITÉRIOS DE ACEITE

8.1. A CONTRATANTE realizará o aceite técnico das atividades considerando:

- execução integral;
- conformidade técnica;
- cumprimento do escopo;
- evidências apresentadas;
- ausência de falhas críticas;
- aderência aos SLAs.

8.2. Atividades rejeitadas deverão ser corrigidas sem ônus adicional.

9. VEDAÇÕES

9.1. Não serão passíveis de medição:

- retrabalho causado pela CONTRATADA;
- correções decorrentes de erro operacional da CONTRATADA;
- indisponibilidades causadas pela CONTRATADA;
- atividades sem evidências;
- atividades sem ordem de serviço;
- atividades não autorizadas.

10. AUDITORIA E RASTREABILIDADE

10.1. A CONTRATANTE poderá auditar, a qualquer tempo:

- logs;
- tickets;
- evidências;
- relatórios;
- trilhas operacionais;
- apontamentos de UST;
- métricas de execução.

A CONTRATADA deverá manter os registros operacionais pelo prazo mínimo de 5 (cinco) anos.

11. DISPOSIÇÕES FINAIS

11.1. Os quantitativos de UST previstos nas ordens de serviço representam estimativas máximas de consumo, não gerando obrigação mínima de contratação.
11.2. As medições deverão observar estritamente os princípios da razoabilidade, proporcionalidade, economicidade, eficiência e interesse público.
11.3. O presente catálogo poderá ser atualizado durante a vigência da Ata de Registro de Preços, mediante justificativa técnica e concordância entre as partes.

ESTUDO TÉCNICO PRELIMINAR
Processo Administrativo n° 031/2026

1. OBJETO

Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA.

2. ÁREA REQUISITANTE

Secretarias dos municípios consorciados ao CP – CISGA.

3. FUNDAMENTAÇÃO

A adoção da modalidade Pregão Eletrônico para Registro de Preços, com critério de julgamento menor preço, fundamenta-se no disposto na Lei nº 14.133/2021, em especial nos arts. 82 a 86, que estabelecem as diretrizes, os pressupostos e as condições para a utilização do Sistema de Registro de Preços no âmbito das contratações públicas.

4. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

No âmbito de suas atribuições finalísticas, o Consórcio Intermunicipal de Desenvolvimento Sustentável da Serra Gaúcha (CISGA) desempenha o papel fundamental de apoiar os municípios consorciados na implementação de medidas que promovam a eficiência administrativa, a inovação tecnológica e a estrita conformidade com as legislações vigentes. No cenário atual, as administrações públicas municipais enfrentam o duplo desafio de acelerar a digitalização de seus processos governamentais e, simultaneamente, mitigar riscos cibernéticos crescentes capazes de paralisar serviços públicos essenciais.

A infraestrutura tecnológica atual das prefeituras é caracterizada por um ambiente altamente heterogêneo de hardware e software, o que pulveriza os pontos de vulnerabilidade e dificulta uma defesa linear e coordenada. Soma-se a isso a crônica escassez de profissionais de TI especializados em segurança da informação nos quadros públicos municipais, impossibilitando que os entes realizem, de forma autônoma, o monitoramento preventivo, a detecção de ameaças em tempo real e a resposta rápida a incidentes de segurança.

O Consórcio é atualmente composto por 25 municípios consorciados. Para fins de levantamento das necessidades relacionadas à segurança da informação e à proteção de dados, foram obtidas respostas de 20 participantes, sendo 19 municípios consorciados e o CISGA.

A partir das informações coletadas, foram identificadas deficiências relevantes na estrutura de segurança da informação e de proteção de dados dos participantes. Verificou-se que 17 municípios

apresentam grau de adequação à Lei Geral de Proteção de Dados (LGPD) classificado como inicial ou inexistente, evidenciando a necessidade de adoção de medidas destinadas ao fortalecimento das práticas de governança e proteção de dados pessoais.

No que se refere às soluções de segurança cibernética, constatou-se que 12 municípios dispõem de Firewall de Próxima Geração, enquanto 12 possuem Antivírus de Próxima Geração. Em relação ao monitoramento da infraestrutura e dos eventos de segurança, apenas 6 municípios contam com soluções de monitoramento NOC/SOC/SIEM. Da mesma forma, somente 6 municípios possuem solução de Backup em Nuvem, demonstrando a existência de lacunas significativas quanto à prevenção, detecção e resposta a incidentes, bem como à continuidade e recuperação dos dados.

O levantamento também permitiu identificar o interesse dos participantes na contratação ou implementação das respectivas soluções. Quanto à Adequação à LGPD, foram registrados 15 municípios interessados. O mesmo número, 15 municípios, manifestou interesse na implantação ou aprimoramento de Firewall de Próxima Geração.

Em relação ao Antivírus de Próxima Geração, 14 municípios demonstraram interesse, enquanto 14 também manifestaram interesse em soluções de monitoramento NOC/SOC/SIEM. Por fim, 15 municípios demonstraram interesse na contratação de solução de Backup em Nuvem.

Dessa forma, os resultados do levantamento evidenciam uma demanda relevante e compartilhada entre os municípios consorciados, especialmente nas áreas de adequação à LGPD, proteção contra ameaças cibernéticas, monitoramento de segurança e realização de backups em nuvem. A diferença entre a estrutura atualmente disponível e o interesse manifestado pelos municípios reforça a existência de necessidade concreta de aprimoramento da infraestrutura de segurança da informação, constituindo elemento relevante para o planejamento de eventual contratação conjunta pelo Consórcio.

A urgência e a indispensabilidade desta contratação conjunta são evidenciadas pelo diagnóstico situacional realizado junto aos municípios consorciados, que revelou um cenário de extrema fragilidade sob duas perspectivas indissociáveis:

a) **Baixa Maturidade em LGPD: 85%** dos municípios respondentes encontram-se em nível de adequação inicial ou inexistente à Lei Geral de Proteção de Dados (Lei nº 13.709/2018), e **nenhum** atingiu o nível avançado. Esta lacuna processual e documental expõe as prefeituras a severas sanções administrativas da ANPD, ações judiciais de titulares de dados e apontamentos pelos órgãos de controle;

b) **Carência de Controles Técnicos de Defesa:** O levantamento de ativos de segurança revelou uma desproteção alarmante no ecossistema de TI dos consorciados:

- Apenas **12 municípios** possuem Firewall de Próxima Geração (NGFW);
- Apenas **12 municípios** possuem Antivírus de Próxima Geração (EDR);
- Apenas **6 municípios** contam com monitoramento ativo (NOC/SOC/SIEM);

- Apenas **6 municípios** dispõem de rotinas de backup em nuvem.

Este diagnóstico comprova que a grande maioria dos consorciados carece de defesas básicas contra ataques de *ransomware*, engenharia social (*phishing*) e invasões de sistemas, que hoje visam especificamente o setor público para sequestro de dados e tentativas de fraudes financeiras e desvios de recursos de contas públicas.

A convergência dessas duas carências, a baixa conformidade jurídica e a fragilidade técnica, exige uma solução integrada.

A adequação à LGPD não se resume à elaboração de termos de consentimento ou políticas de privacidade estáticas. O Artigo 46 da Lei nº 13.709/2018 determina expressamente o seguinte:

> **Art. 46.** Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

Portanto, a conformidade jurídica com a LGPD (representada neste certame pelos Itens 01 a 10) depende umbilicalmente da existência de controles de segurança cibernética ativos (representados pelos Itens 11 a 25). Sem segurança da informação robusta, não há proteção de dados pessoais realizável; sem a governança documental da LGPD, os controles técnicos carecem de conformidade legal.

Diante da impossibilidade de os municípios atraírem e manterem equipes multidisciplinares próprias de segurança cibernética, a contratação adota o modelo de **Provedor de Serviços de Segurança Gerenciados (MSS - *Managed Security Services*)** e de Encarregado de Dados Terceirizado (**DPO *as a Service***).

Trata-se de uma prática amplamente consolidada no setor privado e em expansão na Administração Pública, que permite suprir a lacuna técnica local através da atuação de um parceiro estratégico especializado. A contratação abrangerá uma solução robusta estruturada em três pilares fundamentais:

a) Tecnologia e Proteção:
   a. EDR (Proteção de *Endpoints*);
   b. DLP (Evitar Vazamento);
   c. Gestão de Patches / Backup
b) Serviços Gerenciados:
   a. SOC (*Security Op. Ctr*);

b. SIEM (Correlação Event);
c. Gestão de Vulnerabilidades.

c) Governança e Capacitação:
   a. Mentoria e Treinamento;
   b. DPO as a Service;
   c. Acordos de SLA estritos.

A atuação do MSS garantirá a operação contínua e a otimização dos investimentos de TI já realizados pelos municípios, responsabilizando-se pelo controle de falhas, monitoramento de disponibilidade, análise de desempenho e cumprimento de rigorosos Acordos de Nível de Serviço (SLA), trazendo previsibilidade e economicidade à gestão pública.

A manutenção do atual cenário de vulnerabilidade tecnológica e ausência de adequação legal submete as administrações municipais a riscos concretos e graves, tais como:

a) **Paralisação de Serviços Essenciais:** Ataques de sequestro de dados (*ransomware*) que podem interromper o funcionamento de sistemas de saúde, educação, arrecadação tributária e assistência social por dias ou semanas;
b) **Prejuízos Financeiros e Fraudes:** Exposição a desvios financeiros decorrentes de invasões cibernéticas e fraudes bancárias nos sistemas de pagamentos das prefeituras;
c) **Sanções Administrativas e Judiciais:** Aplicação de sanções administrativas pela Autoridade Nacional de Proteção de Dados (ANPD) e condenações judiciais por vazamento de dados de cidadãos e servidores;
d) **Improbidade Administrativa por Omissão:** Conforme entendimento consolidado dos órgãos de controle, em especial do Tribunal de Contas do Estado do Rio Grande do Sul (TCE-RS), a inércia ou omissão culposa dos gestores em adotar medidas mínimas de conformidade com a LGPD e de proteção do patrimônio digital público caracteriza falha grave de governança, sujeitando os responsáveis à responsabilização administrativa, civil e por eventual ato de improbidade administrativa por negligência na conservação do patrimônio público

Desse modo, resta plenamente caracterizada, justificada e fundamentada a imperiosa necessidade da presente contratação integrada. O projeto não apenas sanará as fragilidades estruturais dos municípios consorciados frente às ameaças cibernéticas e exigências da LGPD, como também promoverá a perenidade administrativa, a segurança jurídica, a responsabilidade fiscal e a proteção integral dos dados de toda a sociedade por eles atendida.

5. ALINHAMENTO ENTRE A CONTRATAÇÃO E A PREVISÃO DA CONTRATAÇÃO NO PLANO ANUAL DE CONTRATAÇÕES - PAC

O presente processo licitatório estará vigente por 12 meses após a homologação. As quantidades foram estimadas para 12 meses de consumo, conforme documento encaminhado pelos municípios participantes, levando em conta a projeção das necessidades futuras.

A contratação pretendida foi aprovada pelos prefeitos dos municípios consorciados ao CISGA na 56ª Assembleia Geral Ordinária de 25 de novembro de 2025, estando, desse modo, alinhada com o planejamento desta Administração para o ano de 2026.

6. REQUISITOS PARA SELEÇÃO DO FORNECEDOR

O fornecedor será selecionado por meio da realização de procedimento de Pregão Eletrônico para Registro de Preço, com critério de julgamento o menor preço. A contratação deve atender a todos os requisitos constantes no Termo de Referência e seus anexos, principalmente no que tange às exigências relativas à descrição dos itens e modelo de Execução do Contrato, bem como o disposto em Edital e demais documentos complementares.

Para a contratação, além dos requisitos técnicos presentes nas descrições dos itens, o fornecedor deve observar os critérios de habilitação jurídica, fiscal, social, trabalhista e econômico-financeira e atender os seguintes requisitos:

Deverá ser apresentado juntamente com a Proposta Final:

a) DECLARAÇÃO DE QUE SUAS PROPOSTAS ECONÔMICAS COMPREENDEM A INTEGRALIDADE DOS CUSTOS para atendimento dos direitos trabalhistas assegurados na Constituição Federal, nas leis trabalhistas, nas normas infralegais, nas convenções coletivas de trabalho e nos termos de ajustamento de conduta vigentes na data de entrega das propostas.

Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Declarações

a) Declaração de que atende aos requisitos de habilitação, e de que o declarante responderá pela veracidade das informações prestadas, na forma da lei (art. 63, I, da Lei nº 14.133/2021);

b) Declaração de Idoneidade (de que não foi declarada inidônea por ato da Administração Pública);

c) Declaração que atende ao disposto no artigo 7°, inciso XXXIII, da Constituição Federal, nos termos do inciso VI do art. 68 da Lei nº 14.133/21;

d) Declaração que não possui empregados executando trabalho degradante ou forçado, observando o disposto nos incisos III e IV do art. 1º e no inciso III do art. 5º da Constituição Federal;

e) Declaração de que cumpre as exigências de reserva de cargos para pessoa com deficiência e para reabilitado da Previdência Social;

f) Declaração da licitante de que não que mantenha vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que desempenhe função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau, conforme art. 14, IV da Lei nº 14.133/2021.

Declaração Exclusiva ME/EPP

a) Declaração de que cumpre os requisitos estabelecidos no artigo 3°da Lei Complementar nº 123, de 2006, estando apto a usufruir do tratamento favorecido estabelecido em seus arts. 42 a 49, observado o disposto nos § 1º ao 3º do art. 4º, da Lei n.º 14.133, de 2021 e observância do limite de R$ 4.800.000,00 na licitação, 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.

Declaração Exclusiva Cooperativa

a) O licitante organizado em Cooperativa deverá apresentar declaração de que cumpre os requisitos estabelecidos no artigo 16 da Lei nº 14.133, de 2021 (modelo em anexo).

Habilitação Jurídica

a) Empresário individual: inscrição no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede;

b) Microempreendedor Individual - MEI: Certificado da Condição de Microempreendedor Individual - CCMEI, cuja aceitação ficará condicionada à verificação da autenticidade no sítio https://www.gov.br/empresas-e-negocios/pt-br/empreendedor;

c) Sociedade empresária, sociedade limitada unipessoal – SLU ou sociedade identificada como empresa individual de responsabilidade limitada - EIRELI: inscrição do ato constitutivo, estatuto ou contrato social no Registro Público de Empresas Mercantis, a cargo da Junta Comercial da respectiva sede, acompanhada de documento comprobatório de seus administradores;

d) Sociedade empresária estrangeira: portaria de autorização de funcionamento no Brasil, publicada no Diário Oficial da União e arquivada na Junta Comercial da unidade federativa

onde se localizar a filial, agência, sucursal ou estabelecimento, a qual será considerada como sua sede, conforme Instrução Normativa DREI/ME n.º 77, de 18 de março de 2020;

e) Sociedade simples: inscrição do ato constitutivo no Registro Civil de Pessoas Jurídicas do local de sua sede, acompanhada de documento comprobatório de seus administradores;

f) Filial, sucursal ou agência de sociedade simples ou empresária: inscrição do ato constitutivo da filial, sucursal ou agência da sociedade simples ou empresária, respectivamente, no Registro Civil das Pessoas Jurídicas ou no Registro Público de Empresas Mercantis onde opera, com averbação no Registro onde tem sede a matriz.

g) Sociedade cooperativa: ata de fundação e estatuto social, com a ata da assembleia que o aprovou, devidamente arquivado na Junta Comercial ou inscrito no Registro Civil das Pessoas Jurídicas da respectiva sede, além do registro de que trata o art. 107 da Lei nº 5.764, de 16 de dezembro 1971.

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

Habilitação fiscal, social e trabalhista

a) Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas (CNPJ) atualizado, relativo ao domicílio ou sede do licitante, pertinente e compatível com o objeto desta licitação;

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

c) Certificado de Regularidade de Situação perante o Fundo de Garantia do Tempo de Serviço, emitido nos moldes do art. 7º, V da Lei nº 8.036, de 11 de maio de 1990;

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

e) Prova de inscrição no cadastro de contribuintes municipal, relativo ao domicilio ou à sede do licitante, pertinente ao seu ramo de atividade e compatível com o objeto Contratual;

f) Certidão de Regularidade com a Fazenda Municipal do domicílio ou sede do licitante, dentro do prazo de validade, na forma da lei;

g) Certidão de Regularidade com a Fazenda Estadual, relativa à atividade em cujo exercício contrata ou concorre, referente ao domicílio da sociedade empresária.

   a. Caso o fornecedor seja considerado isento dos tributos Estaduais relacionados ao objeto contratual, ou isento da inscrição em cadastro estadual de contribuintes, deverá comprovar tal condição mediante a apresentação de declaração da Fazenda respectiva do seu domicílio ou sede, ou outra equivalente, na forma da lei.

   b. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar n. 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

Qualificação Econômico-Financeira

a) Certidão negativa de falência expedida pelo distribuidor do domicílio da sede do fornecedor, Lei nº 14.133, de 2021, art. 69, caput, inciso II).

   a. Se a Certidão de falência não estabelecer prazo de validade, será considerada válida apenas a certidão com prazo de emissão não superior a 90 (noventa) dias da data da sessão.

Qualificação técnica

a) Comprovação de aptidão para execução de serviço de complexidade tecnológica e operacional equivalente ou superior com o objeto desta contratação, ou com o item pertinente, por meio da apresentação de certidões ou atestados, por pessoas jurídicas de direito público ou privado, ou regularmente emitido(s) pelo conselho profissional competente, quando for o caso;

   a. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados e/ou em execução nas seguintes áreas:

      i. Operação de SOC 24x7: Comprovação de fornecimento de serviço de Security Operations Center com monitoramento contínuo, detecção avançada e resposta estendida e coordenada a incidentes;

      ii. Implementação e Operação de Plataforma SIEM: Experiência na implantação, tuning e operação de plataforma de correlação avançada, integrando mais de 50 fontes de dados heterogêneas;

      iii. Projetos de Arquitetura Zero Trust e Controle de Acesso: Implementação de soluções de ZTNA (Zero Trust Network Access);

      iv. Estratégia de Resiliência e Recuperação: Experiência em projetos de Backup Imutável e Disaster Recovery (DR);

v. Implantação e Operação Assistida da Plataforma de Maturidade em segurança da informação.

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

c. Somente serão aceitos atestados expedidos após a conclusão do contrato ou se decorrido, pelo menos, um ano do início de sua execução, exceto se firmado para ser executado em prazo inferior, conforme item 10.8 da IN SEGES/MP n. 5, de 2017;

d. Os atestados ou declarações de capacidade técnica deverão se referir a serviços prestados no âmbito da atividade econômica principal e/ou secundária da licitante, especificada no contrato social devidamente registrado na junta comercial competente, bem como no cadastro de pessoas jurídicas da Receita Federal do Brasil – RFB;

e. Os atestados ou declarações deverão conter as seguintes informações:

i. Nome, CNPJ, dados de endereço e contato da empresa/órgão que emitiu o atestado;

ii. Nome completo e cargo do signatário;

iii. Descrição do serviço de modo a permitir a aferição de sua similaridade com o objeto licitado;

iv. Prazo de execução e quantidade contratada (se aplicável);

v. Período e local da prestação do serviço;

vi. Data de emissão do atestado;

vii. Assinatura do representante do órgão atestante.

b) Comprovação de possuir em seu quadro permanente, na data da licitação, ou compromisso de contratação, equipe técnica multidisciplinar com profissionais das seguintes áreas:

a. 01 Analista de sistemas.

i. Nível superior completo em áreas da Tecnologia da Informação.

b. 01 Advogado.

i. Nível superior completo em direito com registro na OAB.

c. 01 Analista de requisitos.

i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito.

ii. Título de especialização em engenharia de sistemas para web, gestão empresarial ou áreas afins.

d. 01 Analista de Segurança da informação;

i. Nível superior completo na área de Segurança da Informação.

e. 01 Analista de Governança Corporativa;
   i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;
   ii. Título de especialização em governança corporativa e risco, ou áreas afins;
   iii. Certificação Lead Assessor SIG ISO 37301:2021 – Gestão em Compliance – Requisitos com orientações para uso;
   iv. Certificação Lead Assessor SIG ISO 31000:2009 e ISO 22301:2019 – Gestão de Riscos e Continuidade de Negócios.

f. 01 Encarregado de Dados (DPO).
   i. Nível superior completo nas áreas relacionadas a tecnologia, administração, comunicação, contabilidade ou direito;
   ii. Certificação como Lead Assessor ISO 27001:2022 e ISO 27701:2019 – Gestão da Segurança da Informação e Gestão de Privacidade da Informação;
   iii. Certificação Data Protection Officer – DPO;

c) Prova que a empresa possui vínculo com os profissionais indicados por meio de da apresentação de contrato social, em se tratando de sócio da empresa; mediante cópia da Carteira de Trabalho e Previdência Social – CTPS, no caso de empregado; por meio de contrato de prestação de serviços; ou através de declaração de contratação futura do profissional.

d) No caso de apresentação de Declaração de Contratação futura do profissional, esta deve ser acompanhada de declaração de anuência do profissional, **devidamente assinada**.

7. DO LEVANTAMENTO DE MERCADO

O mercado de soluções de adequação à LGPD, segurança cibernética e backup em nuvem oferece diversas alternativas. Para a presente contratação, as soluções disponíveis foram analisadas com base nos seguintes critérios: compatibilidade com o modelo de contratação por Ata de Registro de Preços, capacidade de atendimento a múltiplos municípios de portes distintos e viabilidade de fornecimento na modalidade de serviços gerenciados com regime de comodato.

A pesquisa de mercado será realizada por meio de cotação com fornecedores do Estado, adotando-se o critério de menor preço global porá o lote, em conformidade com a modalidade de Pregão Eletrônico prevista para o certame. As cotações serão formalizadas mediante solicitação de orçamento a, no mínimo, três empresas especializadas nos ramos de consultoria em privacidade de dados, segurança cibernética e serviços de backup em nuvem, conforme diretrizes da Lei nº 14.133/2021.

Os orçamentos coletados serão consolidados em planilha própria e integrarão os autos do processo administrativo.

8. DA DESCRIÇÃO DA SOLUÇÃO COMO UM TODO

A solução proposta consiste na contratação, por meio de **Ata de Registro de Preços**, de empresa especializada para fornecimento, implantação, licenciamento, subscrição, operação assistida, treinamento e suporte técnico de soluções integradas de governança, privacidade, proteção de dados, segurança cibernética, continuidade operacional e monitoramento de infraestrutura tecnológica.

A contratação destina-se aos municípios consorciados e ao próprio CISGA, permitindo que cada órgão ou entidade participante realize a contratação dos itens de acordo com sua necessidade efetiva, disponibilidade orçamentária, porte populacional, quantidade de ativos, volume de dados, criticidade dos serviços e nível de maturidade em segurança da informação e proteção de dados.

A solução deverá ser composta pelos itens descritos na tabela do item 1.2 deste Termo de Referência, organizados nos seguintes blocos funcionais integrados e complementares.

Governança, adequação e manutenção da conformidade com a LGPD — Itens 01 a 07

Os Itens 01 a 07 compreendem a implantação e o licenciamento de software para adequação à Lei Geral de Proteção de Dados Pessoais — LGPD, bem como a terceirização do Encarregado pelo Tratamento de Dados Pessoais, conforme os tipos de atendimento definidos para os municípios participantes.

A solução deverá contemplar, conforme o tipo contratado:

- Diagnóstico do nível de maturidade em privacidade e proteção de dados;
- Identificação dos agentes de tratamento e das responsabilidades institucionais;
- Inventário de dados pessoais e dados pessoais sensíveis;
- Mapeamento dos processos e das operações de tratamento;
- Registro das Operações de Tratamento de Dados Pessoais — ROPA;
- Identificação das bases legais aplicáveis;
- Avaliação de riscos de privacidade;
- Elaboração e atualização de Relatórios de Impacto à Proteção de Dados Pessoais — RIPD;
- Elaboração e revisão de políticas, normas e procedimentos;
- Apoio à gestão de incidentes envolvendo dados pessoais;
- Apoio ao atendimento das solicitações dos titulares;
- Gestão de planos de ação e não conformidades;
- Treinamento e conscientização de servidores e colaboradores;
- Disponibilização de plataforma para gestão, acompanhamento e comprovação das ações de adequação;

- Atuação do Encarregado como canal de comunicação entre o controlador, os titulares e a Autoridade Nacional de Proteção de Dados — ANPD, quando aplicável.

Os Itens 02 a 09 deverão ser dimensionados conforme o tipo de município ou órgão contratante, considerando porte, população, estrutura administrativa, quantidade de unidades, número de servidores, complexidade dos tratamentos e volume de dados pessoais tratados.

O Item 01 compreenderá as atividades de implantação do software para adequação à LGPD nos Tipos I, II, III, IV e V, incluindo planejamento, parametrização, configuração, cadastramento inicial, integração, capacitação e entrega da documentação necessária ao início da operação.

Plataforma unificada de segurança cibernética — Itens 08 e 09

O Item 08 compreende o fornecimento de plataforma unificada de segurança cibernética, com setup, implantação e suporte pelo período de 12 meses, abrangendo, conforme aplicável, os seguintes módulos e capacidades:

- Segurança de ambientes de nuvem;
- Segurança de correio eletrônico;
- Segurança de endpoints;
- Governança de dados em endpoints;
- Governança e proteção de dados;
- Segurança de redes;
- Gestão de equipamentos móveis — MDM;
- Detecção e resposta em endpoints — EDR;
- Inbound Gateway;
- Secure Web Gateway;
- Proteção contra phishing, inclusive em redes sem fio;
- Segurança de mensagens;
- Conscientização e treinamento de usuários;
- Automação inteligente de tarefas de segurança;
- Geração de alertas, relatórios e indicadores;
- Integração com SIEM, SOC, NOC, RMM, DLP, firewall e demais soluções contratadas.

A plataforma deverá permitir o gerenciamento centralizado das políticas de segurança, a identificação de comportamentos suspeitos, a aplicação de medidas preventivas e corretivas e a integração dos controles de proteção de usuários, endpoints, redes, aplicações, nuvem e dados.

O Item 09 compreenderá a operação assistida e o treinamento para utilização da plataforma unificada, incluindo apoio à configuração de políticas, parametrização de regras, criação de perfis, análise de alertas, execução de procedimentos operacionais, elaboração de documentação e transferência de conhecimento às equipes da CONTRATANTE.

Detecção e resposta a incidentes em endpoints — Itens 10 e 11

O Item 10 compreende o fornecimento de solução de **Endpoint Detection and Response — EDR**, com setup, implantação e suporte durante 12 meses, destinada à detecção, investigação e resposta a incidentes de segurança em estações de trabalho, notebooks, servidores e demais endpoints contratados.

A solução deverá contemplar, no mínimo:

- Monitoramento de processos, arquivos, conexões e atividades dos endpoints;
- Detecção baseada em comportamento, indicadores de comprometimento e inteligência de ameaças;
- Identificação de malware, ransomware, exploração de vulnerabilidades e movimentação lateral;
- Isolamento remoto de endpoints comprometidos;
- Bloqueio ou encerramento de processos maliciosos;
- Quarentena de arquivos;
- Coleta de evidências;
- Investigação de incidentes;
- Busca retrospectiva de ameaças;
- Trilhas de auditoria;
- Relatórios técnicos e gerenciais;
- Integração com SIEM, SOC, antiransomware, RMM e demais soluções de segurança.

O Item 11 compreenderá a operação assistida e o treinamento da solução EDR, incluindo configuração, ajuste de políticas, análise de alertas, apoio à investigação, execução de ações autorizadas de contenção, elaboração de procedimentos e capacitação das equipes da CONTRATANTE.

Proteção e prevenção contra vazamento de dados — Itens 12 e 13

O Item 12 compreende o fornecimento de solução de **Data Loss Prevention — DLP**, com setup, implantação e suporte durante 12 meses, destinada à prevenção, detecção e tratamento de tentativas de acesso, cópia, transferência, compartilhamento ou exfiltração indevida de informações.

A solução deverá proteger, conforme o escopo contratado:

- Dados em uso;

- Dados em trânsito;
- Dados armazenados;
- Endpoints;
- Correio eletrônico;
- Navegação web;
- Dispositivos removíveis;
- Aplicações em nuvem;
- Compartilhamento de arquivos;
- Impressões e cópias;
- Informações classificadas ou sensíveis.

Deverá permitir a definição de políticas baseadas em conteúdo, contexto, usuário, dispositivo, aplicação, localização e comportamento, bem como a geração de alertas, bloqueios, registros, relatórios e evidências para investigação.

O Item 13 compreenderá a operação assistida e o treinamento da solução DLP, incluindo apoio à classificação de dados, criação e ajuste de políticas, gestão de exceções, análise de eventos, tratamento de incidentes e transferência de conhecimento.

Gerenciamento e correlação de eventos de segurança — Item 14

O Item 14 compreende o fornecimento de software de **Security Information and Event Management — SIEM**, com setup, implantação e suporte pelo período de 12 meses, destinado à coleta, normalização, correlação, retenção, análise e consulta de eventos de segurança.

A solução deverá permitir:

- Integração com firewalls, EDR, DLP, RMM, antivírus, servidores, sistemas operacionais, aplicações, bancos de dados, dispositivos de rede e soluções em nuvem;
- Coleta e normalização de logs;
- Correlação de eventos provenientes de múltiplas fontes;
- Criação, manutenção e revisão de casos de uso;
- Detecção de comportamentos anômalos;
- Geração de alertas;
- Investigação de incidentes;
- Preservação de trilhas de auditoria;
- Controle de acesso e segregação de funções;
- Retenção e consulta de eventos;
- Integração com SOC, NOC e ferramentas de orquestração e resposta;

- Emissão de relatórios técnicos, operacionais e executivos.

O dimensionamento deverá considerar a quantidade de ativos monitorados, o volume de eventos, a taxa de ingestão, os requisitos de retenção e a criticidade dos ambientes.

Avaliação de riscos e gestão de maturidade em segurança — Itens 15 e 16

O Item 15 compreende o fornecimento de software para avaliação de riscos, gestão de maturidade e acompanhamento da postura de segurança cibernética, com setup, implantação e suporte por 12 meses.

A solução deverá ser fundamentada, quando aplicável, em referências reconhecidas, incluindo:

- NIST Cybersecurity Framework;
- NIST Risk Management Framework;
- CIS Controls;
- ISO/IEC 27001;
- ISO/IEC 27002;
- Avaliação do nível de maturidade;
- Identificação de riscos e lacunas de controle;
- Classificação e priorização de riscos;
- Registro de evidências;
- Elaboração de planos de tratamento;
- Acompanhamento de responsáveis e prazos;
- Medição da evolução da maturidade;
- Geração de indicadores;
- Emissão de relatórios técnicos e executivos;
- Apoio à conformidade legal, normativa e institucional.

O Item 16 compreenderá a operação assistida e o treinamento para utilização da solução, incluindo apoio à parametrização dos frameworks, cadastramento de controles, avaliação de riscos, definição de planos de ação, acompanhamento de evidências e capacitação das equipes.

Backup resiliente e recuperação de desastre — Itens 17 e 28

O Item 17 compreende o fornecimento de sistema de backup resiliente, com capacidade de recuperação por meio de **Disaster Recovery — DR Online**, setup, implantação e suporte durante 12 meses.

A solução deverá contemplar, no mínimo:

- Execução automatizada de cópias de segurança;
- Armazenamento segregado e externo;

- Criptografia dos dados em trânsito e em repouso;
- Proteção contra exclusão, alteração ou criptografia indevida;
- Imutabilidade das cópias, quando aplicável;
- Políticas de retenção configuráveis;
- Controle de integridade;
- Restauração de arquivos, pastas, sistemas, máquinas virtuais e servidores;
- Recuperação de ambientes críticos;
- Replicação para ambiente de contingência;
- Monitoramento das rotinas;
- Relatórios de sucesso, falha e utilização;
- Testes periódicos de restauração;
- Definição e acompanhamento de requisitos de RTO e POR.

O dimensionamento será realizado com base na quantidade de terabytes protegidos, na criticidade dos dados, nos períodos de retenção e nas necessidades de recuperação dos participantes.

O Item 18 compreenderá a operação assistida e o treinamento da solução de backup e DR Online, incluindo configuração de políticas, acompanhamento das rotinas, análise de falhas, testes de restauração, atualização dos procedimentos e capacitação dos responsáveis técnicos.

Centro de Operações de Segurança — SOC — Itens 19 e 20

Os Itens 19 e 20 compreendem a contratação de serviço de **Security Operations Center — SOC**, com setup, implantação e suporte durante 12 meses, nos modelos:

- **SOC 8x5**, com atendimento durante oito horas por dia e cinco dias por semana; e
- **SOC 24x7**, com atendimento ininterrupto, 24 horas por dia, sete dias por semana e 365 dias por ano.

A escolha do modelo de operação deverá ficar a critério da CONTRATANTE, considerando a criticidade dos serviços, o nível de exposição, os requisitos de continuidade e a necessidade de monitoramento e resposta fora do horário comercial.

O SOC deverá contemplar, conforme o modelo contratado:

- Coleta, recebimento, normalização e correlação de eventos;
- Monitoramento de ativos, redes, endpoints, usuários, identidades, aplicações e ambientes em nuvem;
- Triagem e classificação de alertas;
- Investigação de incidentes;
- Identificação de indicadores de comprometimento;

- Detecção de malware, ransomware, phishing, exfiltração, movimentação lateral e elevação indevida de privilégios;
- Notificação e escalonamento dos incidentes;
- Apoio à contenção e à resposta;
- Preservação de evidências;
- Elaboração de relatórios técnicos e gerenciais;
- Manutenção de casos de uso e regras de detecção;
- Indicadores de desempenho e cumprimento de SLA;
- Integração com SIEM, EDR, DLP, firewall, RMM, antiransomware e demais soluções.

O dimensionamento dos Itens 19 e 20 deverá ser realizado por ativos monitorados, considerando a quantidade de fontes de eventos, o volume de registros, a criticidade dos ambientes, o regime de operação e os níveis de serviço definidos no Termo de Referência.

Monitoramento e gerenciamento remoto de ativos de TI — Itens 21 e 22

O Item 21 compreende o fornecimento de solução de **Remote Monitoring and Management — RMM**, com setup, implantação e suporte durante 12 meses, destinada ao monitoramento, gerenciamento e administração remota de endpoints, servidores, notebooks, dispositivos móveis, quando suportados, e demais ativos de TI previstos na contratação.

A solução deverá permitir:

- Inventário automatizado de hardware e software;
- Monitoramento de disponibilidade;
- Monitoramento de CPU, memória, armazenamento e rede;
- Monitoramento de serviços e processos;
- Geração de alertas;
- Aplicação remota de atualizações;
- Gestão de patches;
- Execução controlada de scripts;
- Automação de tarefas recorrentes;
- Manutenção preventiva e corretiva;
- Suporte remoto;
- Aplicação de políticas de configuração;
- Apoio à identificação de vulnerabilidades;
- Distribuição remota de software;

- Registro e rastreabilidade das ações;
- Integração com ITSM, SIEM, EDR, DLP, SOC e demais ferramentas.

O Item 22 compreenderá a operação assistida e o treinamento da solução RMM, incluindo implantação de agentes, configuração de políticas, criação de automações, elaboração de scripts, tratamento de alertas, uso do acesso remoto, gestão de inventário e capacitação das equipes da CONTRATANTE.

Proteção contra ransomware, descriptografia e detecção de exfiltração — Itens 23 e 24

O Item 23 compreende a contratação de ferramenta de proteção contra ransomware, com capacidade de detecção de exfiltração de dados e, quando tecnicamente possível, recursos de descriptografia, setup, implantação e suporte durante 12 meses.

A solução deverá contemplar:

- Detecção de comportamento associado a ransomware;
- Identificação de tentativas de criptografia maliciosa;
- Proteção de arquivos, diretórios, servidores e endpoints;
- Bloqueio de processos suspeitos;
- Isolamento de ativos comprometidos;
- Identificação de movimentação lateral;
- Detecção de exfiltração de dados;
- Monitoramento de alterações anômalas;
- Recuperação ou reversão de arquivos, quando suportado;
- Recursos de descriptografia, quando disponíveis para a ameaça identificada;
- Geração de alertas e evidências;
- Integração com EDR, SIEM, SOC, DLP e backup resiliente.

O Item 24 compreenderá a operação assistida e o treinamento da ferramenta, incluindo configuração das políticas, análise de alertas, tratamento de incidentes, realização de testes, definição de procedimentos de contenção e capacitação dos responsáveis.

Arquitetura Zero Trust, microsegmentação e ofuscação — Itens 25 e 26

O Item 25 compreende o fornecimento de solução de software baseada em princípios de **Zero Trust**, destinada à microsegmentação, controle de comunicação e ofuscação de ativos, com setup, implantação e suporte durante 12 meses.

A solução deverá possibilitar:

- Aplicação do princípio de nunca confiar, sempre verificar;
- Controle de acesso baseado em identidade, dispositivo, aplicação e contexto;

- Microsegmentação de redes e cargas de trabalho;
- Restrição de movimentação lateral;
- Controle de comunicação entre aplicações e serviços;
- Isolamento de ambientes críticos;
- Redução da exposição de ativos;
- Ofuscação de serviços e componentes;
- Aplicação do menor privilégio;
- Monitoramento de fluxos;
- Criação de políticas de comunicação;
- Registro e auditoria das ações;
- Integração com identidade, firewall, EDR, SIEM e SOC.

O Item 26 compreenderá a operação assistida e o treinamento da solução Zero Trust, incluindo levantamento de fluxos, definição de políticas, implantação gradual, validação em ambiente piloto, ajustes, documentação e transferência de conhecimento.

Centro de Operações de Rede — NOC — Item 27

O Item 27 compreende a contratação de serviço de **Network Operations Center — NOC**, em regime 24x7, 365 dias por ano, com setup, implantação e suporte durante 12 meses.

O NOC deverá realizar o monitoramento contínuo da infraestrutura de rede e dos ativos contratados, abrangendo, quando aplicável:

- Links de comunicação;
- Roteadores;
- Switches;
- Firewalls;
- Controladores;
- Pontos de acesso;
- Servidores;
- Interfaces;
- Túneis VPN;
- Dispositivos de conectividade;
- Equipamentos e serviços críticos;
- Monitoramento de disponibilidade;
- Monitoramento de desempenho;
- Acompanhamento de latência, perda de pacotes e utilização;

- Identificação de falhas e degradações;
- Abertura e acompanhamento de chamados;
- Acionamento de operadoras e terceiros;
- Escalonamento técnico;
- Apoio à análise de causa;
- Registro das ocorrências;
- Relatórios de disponibilidade e desempenho;
- Indicadores de capacidade e continuidade;
- Integração com SOC, SIEM, RMM e ferramentas de gestão de serviços.

O dimensionamento deverá ser realizado por ativos monitorados, considerando a quantidade, a criticidade, a distribuição geográfica, os níveis de redundância e os requisitos de disponibilidade dos participantes.

Segurança de rede por meio de firewalls NGFW — Itens 28 a 31

Os Itens 28 a 31 compreendem o fornecimento de equipamentos de segurança de redes do tipo **Next Generation Firewall — NGFW**, nos Modelos I, II, III e IV, com setup, implantação e suporte durante 12 meses.

Os equipamentos deverão ser dimensionados conforme o porte, a capacidade de processamento, o volume de tráfego, a quantidade de usuários, a quantidade de conexões, a quantidade de unidades remotas e a criticidade do ambiente de cada participante.

A solução deverá contemplar, conforme o modelo contratado:

- Firewall de próxima geração;
- Controle de aplicações;
- Sistema de prevenção contra intrusão — IPS;
- Antimalware de rede;
- Filtragem web;
- Inspeção de tráfego criptografado;
- VPN site-to-site;
- VPN para acesso remoto;
- Alta disponibilidade, quando prevista;
- Controle de usuários e grupos;
- Políticas de segurança;
- Registro e análise de logs;
- Integração com gerenciamento centralizado;

- Atualização de firmware;
- Atualização de assinaturas;
- Monitoramento de desempenho;
- Suporte técnico;
- Substituição de equipamento defeituoso, conforme SLA.

A implantação deverá compreender instalação física ou lógica, configuração inicial, parametrização das políticas, integração com a rede existente, testes de funcionamento, documentação e entrega do ambiente em condições operacionais.

Criptografia, anonimização, custódia e rastreabilidade documental — Itens 32 a 37

O Item 32 compreende a contratação de subscrição anual de plataforma em nuvem para criptografia, anonimização, custódia e rastreabilidade documental, por município ou órgão participante.

A plataforma deverá permitir, conforme o escopo contratado:

- Criptografia de documentos e arquivos;
- Anonimização de informações;
- Custódia cifrada;
- Armazenamento protegido;
- Controle de acesso;
- Gestão de permissões;
- Registro de operações;
- Rastreabilidade de acessos e alterações;
- Marcação de páginas ou documentos;
- Preservação de evidências;
- Consulta a trilhas de auditoria;
- Geração de relatórios;
- Gestão de usuários e perfis;
- Integração com sistemas e repositórios institucionais.

Os Itens 33 a 36 compreendem créditos excedentes às franquias contratadas para Anonimização de páginas equivalentes, Custódia cifrada de arquivos, Armazenamento adicional e Rastreabilidade de páginas marcadas.

A utilização desses créditos deverá ser registrada, mensurada e apresentada nos relatórios de consumo, permitindo o acompanhamento da capacidade contratada e da utilização efetiva por município ou órgão.

O Item 37 compreenderá a operação assistida e o treinamento para os Itens 32 a 36, incluindo configuração da plataforma, criação de perfis, definição de políticas, utilização dos créditos, anonimização, custódia, armazenamento, rastreabilidade, geração de relatórios e capacitação dos usuários e administradores.

Integração entre os componentes da solução

A integração entre os itens deverá proporcionar uma arquitetura coordenada de proteção, governança, monitoramento, resposta e recuperação.

A governança de privacidade e a adequação à LGPD, previstas nos Itens 01 a 07, deverão ser apoiadas por medidas técnicas e administrativas relacionadas à proteção de endpoints, redes, dados, identidades e ambientes em nuvem.

A plataforma unificada, o EDR, o DLP, o SIEM, o SOC, o RMM, o antiransomware, o Zero Trust, o NOC e os firewalls deverão atuar de forma complementar, permitindo:

- Maior visibilidade sobre os ativos e eventos;
- Correlação de informações provenientes de diferentes camadas;
- Redução do tempo de detecção e resposta;
- Aplicação coordenada de contramedidas;
- Proteção contra ameaças internas e externas;
- Redução da movimentação lateral;
- Prevenção de vazamento e exfiltração;
- Preservação de evidências;
- Melhoria da capacidade de auditoria;
- Apoio à continuidade dos serviços públicos.

O backup resiliente e a recuperação de desastre, previstos nos Itens 17 e 18, deverão complementar os controles de prevenção e resposta, assegurando a recuperação dos dados e sistemas em situações de falha, indisponibilidade, desastre ou ataque cibernético.

A plataforma de criptografia, anonimização, custódia e rastreabilidade documental, prevista nos Itens 32 a 37, deverá complementar a proteção dos dados tratados pelos municípios e órgãos, fortalecendo o controle sobre documentos, informações pessoais, arquivos institucionais e evidências administrativas.

Implantação, operação assistida, treinamento e suporte

A implantação das soluções deverá ser realizada de forma planejada e gradual, considerando:

- Diagnóstico do ambiente;
- Levantamento de requisitos;

- Definição do plano de implantação;
- Identificação das dependências;
- Configuração inicial;
- Integração com sistemas existentes;
- Testes funcionais e de segurança;
- Validação pela CONTRATANTE;
- Documentação;
- Treinamento;
- Entrada em produção;
- Acompanhamento assistido;
- Correção de não conformidades.

Os serviços de operação assistida e treinamento deverão promover a transferência de conhecimento às equipes da CONTRATANTE, sem afastar a responsabilidade da CONTRATADA de manter equipe técnica qualificada e em quantidade suficiente para cumprir os níveis de serviço contratados.

A CONTRATADA deverá disponibilizar suporte técnico, canais de atendimento, procedimentos de escalonamento, registros de chamados, acompanhamento de incidentes e relatórios periódicos, observando os níveis de serviço estabelecidos no Termo de Referência.

Dimensionamento individualizado e caráter estimativo

Os quantitativos registrados na Ata possuem natureza estimativa e constituem limite máximo para futuras contratações. Cada adesão ou contratação decorrente deverá ser dimensionada individualmente, considerando.

- Porte e estrutura do município ou órgão;
- Quantidade de endpoints;
- Quantidade de ativos monitorados;
- Número de usuários;
- Número de servidores;
- Quantidade de unidades administrativas;
- Volume de dados;
- Volume de logs e eventos;
- Quantidade de links e equipamentos de rede;
- Criticidade dos serviços;
- Necessidades de continuidade;

- Nível de maturidade;
- Disponibilidade orçamentária;
- Modelo de operação escolhido.

A contratação efetiva ficará condicionada à necessidade da Administração, à emissão do instrumento correspondente, à disponibilidade orçamentária e ao cumprimento dos procedimentos de gestão e fiscalização.

A previsão dos quantitativos não obriga a CONTRATANTE ao consumo integral dos itens registrados, mas proporciona flexibilidade para atender à expansão do ambiente, à adesão de participantes, à evolução tecnológica e a necessidades supervenientes durante a vigência da Ata.

Responsabilidade pela operação integrada

A CONTRATADA deverá assegurar que os componentes fornecidos sejam tecnicamente compatíveis, interoperáveis e capazes de operar de forma integrada, quando essa integração estiver prevista no escopo contratado.

Deverá também manter documentação atualizada da arquitetura, dos fluxos de integração, das políticas, das configurações, dos procedimentos de operação, dos contatos de escalonamento e das responsabilidades de cada equipe.

A solução deverá ser orientada pelos princípios de defesa em profundidade, menor privilégio, segregação de funções, rastreabilidade, continuidade, prevenção, detecção, resposta e recuperação, permitindo que os municípios consorciados e o CISGA elevem sua maturidade em privacidade, segurança cibernética e gestão de infraestrutura tecnológica.

9. DAS QUANTIDADES ESTIMADA

ITEM	**Contratação de soluções de adequação à lei geral de proteção de dados (LGPD), serviços gerenciados de segurança cibernética, backup em nuvem e suporte técnico especializado, compreendendo serviço de adequação à LGPD e manutenção recorrente, firewalls de próxima geração (NGFW), gerenciamento centralizado e retenção de logs, serviço gerenciado de monitoramento e resposta a incidentes (NOC/SOC/SIEM), software de antivírus com VPN/ZTNA, backup em nuvem, transceivers, treinamento e horas técnicas de suporte especializado, para atender às necessidades demandadas pelos municípios consorciados ao CP – CISGA**.	UNIDADE	QUANTIDADE ESTIMADAS
01	Implantação do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I, II, III.	UST (unidade)	20.208
02	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo I	Até 30.00 Habi-tantes (mês)	192

03	Terceirização do Encarregado de Dados – Tipo I	Até 30.000 Habitantes (mês)	192
04	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo II	De 30.001 até 50.000 habitantes (mês)	36
05	Terceirização do Encarregado de Dados – Tipo II	De 30.001 até 50.000 habitantes (mês)	36
06	Licença do Software para adequação à lei geral de proteção de dados – LGPD – Tipo III	De 50.001 até 100.000 habitantes (mês)	12
07	Terceirização do Encarregado de Dados – Tipo III	De 50.001 até 100.000 habitantes (mês)	12
08	Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
09	Operação Assistida e Treinamento para Plataforma unificada de segurança cibernética para Segurança de Nuvem, Segurança de E-mail, Segurança de Endpoint, Governança de Dados em Endpoints, Governança de Dados, Segurança de Rede, Gestão de Equipamentos Móveis (MDM), Endpoint Detection and Response (EDR), Inbound Gateway, Secure Web Gateway, Wi-Fi Phishing, Segurança de Mensagens e Conscientização de Segurança com automação inteligente.	UST (unidade)	7.680
10	Solução de Detecção e Resposta a Incidentes em Endpoints (EDR) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
11	Operação Assistida e Treinamento para Solução de Detecção e Resposta a Incidentes em Endpoints (EDR)	UST (unidade)	7.680
12	Solução de Proteção e Prevenção de Vazamento de Dados (DLP) com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
13	Operação Assistida e Treinamento para Solução de Proteção e Prevenção de Vazamento de Dados (DLP).	Endpoint (unidade)	7.680
14	Software de SIEM - Security Information&Event Managment com setup/implantação e suporte de 12 meses.	Ativo Monitorado (unidade)	3.552
15	Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos,	Endpoint (unidade)	68.928

	conformidade, maturidade com setup/implantação e suporte de 12 meses.		
16	Operação Assistida e Treinamento para Software de Avaliação de Risco, Gestão de Maturidade em Segurança, fundamentado nos frameworks NIST, CIS Controls e ISO/IEC 27001. contra ataques cibernéticos, conformidade, maturidade.	UST (unidade)	7.680
17	Sistema de Backup Resilente, recuperação via DR Online com setup/implantação e suporte de 12 meses.	TB Protegido (unidade)	2.604
18	Operação Assistida e Treinamento para Sistema de Backup Resilente, recuperação via DR Online.	UST (unidade)	7.680
19	SOC - Security Operations Center – 8x5 com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	39.192
20	SOC - Security Operations Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	33.288
21	Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM), com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
22	Operação Assistida e Treinamento para Solução de Monitoramento e Gerenciamento Remoto de Ativos de TI (RMM).	UST (unidade)	7.680
23	Contratação de Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados de ransomware com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
24	Operação Assistida e Treinamento para Ferramenta de antiransomware, descriptografia e ferramenta de detecção de exfiltração de dados.	UST (unidade)	7.680
25	Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação com setup/implantação e suporte de 12 meses.	Endpoint (unidade)	68.928
26	Operação Assistida e Treinamento para Soluçao de Software Zero Trust (Confiança Zero) para Microsegmentação e Ofuscação.	UST (unidade)	7.680
27	NOC – Network Operation Center – 24x7, 365 dias por ano com setup/implantação e suporte de 12 meses.	Ativos monito-rados (unidade)	3.552
28	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo I com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	5
29	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo II com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	12
30	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo III com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	6
31	Contratação de equipamentos de segurança de redes do tipo firewall de próxima geração — NGFW modelo IV com setup/implantação e suporte de 12 meses.	Equipamento (unidade)	5

32	Subscrição anual de plataforma em nuvem de criptografia, anonimização e rastreabilidade documental.	Subscrição anual por municí-pio/Orgao (mês)	240
33	Crédito de anonimização excedente à franquia	Mil páginas equivalentes (unidade)	303
34	Crédito de custódia cifrada excedente à franquia	Mil arquivos (unidade)	125
35	Crédito de armazenamento excedente à franquia	Gigabyte (unidade)	1.485
36	Crédito de rastreabilidade excedente à franquia	Mil Páginas Marcadas (unidade)	157
37	Operação Assistida e Treinamento para itens – 33 ao 36	UST (unidade)	7.680

10. DOS LOCAIS DE PRESTAÇÃO DOS SERVIÇOS

O prazo e os locais, preliminares, das prestações dos serviços estão devidamente especificados nos Documentos de Formalização da Demanda encaminhados pelos municípios consorciados e, da mesma forma, estarão dispostos em anexo ao edital.

11. DA NATUREZA DA CONTRATAÇÃO

Os serviços a serem contratados compreendem solução integrada de natureza técnica, com componentes de caráter intelectual, intangível e indivisível, cujos padrões de desempenho e qualidade podem ser objetivamente definidos no Termo de Referência, por meio de especificações usuais de mercado.

Quanto à sua natureza, trata-se de um certame destinado à contratação de serviços comuns, que serão adquiridos por meio de licitação, na modalidade pregão eletrônico. O fornecimento da solução descrita no objeto não envolve tecnologias inovadoras ou técnicas desconhecidas no mercado, sendo passível de execução com recursos e práticas amplamente disponíveis.

O conceito formal de bem e serviço comum está definido no art. 6º, inciso XIII, da Lei nº 14.133/2021. Vejamos:

> Art. 6º Para os fins desta Lei, consideram-se:
>
> XIII - bens e serviços comuns: aqueles cujos padrões de desempenho e qualidade podem ser objetivamente definidos pelo edital, por meio de especificações usuais de mercado;

> O Art. 2º do Decreto nº 10.818, de 27 de setembro de 2021, também classifica os bens comuns, conforme segue:
>
> II - bem de qualidade comum - bem de consumo com baixa ou moderada elasticidade-renda da demanda.

Os serviços não infringem o Decreto nº 9.507/2018, pois não envolvem tomadas de decisão ou posicionamento institucional nas áreas de planejamento, coordenação, supervisão e controle; não colocam em risco o controle de processos e de conhecimentos e tecnologias; não são inerentes às categorias funcionais abrangidas pelo plano de cargos do órgão ou entidade; e, por fim, compreendem somente os serviços auxiliares, instrumentais ou acessórios do órgão ou entidade contratante.

12. DA CONTINUIDADE DO SERVIÇO

Inicialmente, cumpre destacar que não há na Lei 14.133 uma definição acerca do que se entende por serviço contínuo. Dada a inércia, devemos nos balizar perante os entendimentos doutrinário e jurisprudencial. Nesse sentido, recorre-se a orientação do TCU[1]:

> Serviços de natureza contínua são serviços auxiliares e necessários à Administração no desempenho das respectivas atribuições. São aqueles que, se interrompidos, podem comprometer a continuidade de atividades essenciais e cuja contratação deva estender-se por mais de um exercício financeiro.
> Em processo próprio, deve a Administração definir e justificar quais outros serviços contínuos necessitam para desenvolver as atividades que lhe são peculiares.

O serviço objeto deste estudo decorre da prestação do serviço de *software* para adequação com a LGBD, mediado pela concessão de licença de uso. Assim os entes participantes desta contratação têm a obrigação de cumprir a legislação, tanto no que diz respeito à sua criação e funcionamento quanto às atividades que realizam.

Desse modo, o serviço é enquadrado como continuado, tendo em vista que tem como objetivo atender à necessidade pública de forma permanente e contínua. Ademais a vigência plurianual poderá ser mais vantajosa considerando a economia de escala viabilizada através da amortização dos custos da contratação durante a vigência além de um exercício.

[1] Brasil. Tribunal de Contas da União. Licitações e contratos: orientações e jurisprudência do TCU. 4. ed. rev., atual. e ampl. – Brasília: TCU, Secretaria-Geral da Presidência: Senado Federal, Secretaria Especial de Editoração e Publicações, 2010. p. 772.

13. DA ESTIMATIVA DO VALOR DA CONTRATAÇÃO

A pesquisa de preços é um processo obrigatório que antecede as contratações da Administração e que define o valor estimado a ser gasto com a contratação pretendida. Ela é vital para auxiliar a Administração na obtenção da proposta mais vantajosa. Isto porque uma pesquisa mal executada é sempre prejudicial ao processo, uma estimativa de preços muito baixa aumenta a ocorrência de licitações desertas; uma estimativa muito alta, compromete a economicidade da aquisição do serviço desejado.

Evidencia-se que o preço de referência deve refletir o preço de mercado, levando em consideração todos os fatores que influenciam na formação dos custos. Alguns desses fatores são: especificação do bem ou serviço, quantidade adquirida, praça ou mercado a ser pesquisado (municipal, estadual, nacional ou internacional), prazos de entrega, forma de execução e modalidade de compra (compra direta, dispensa de licitação, pregão, outros).

A jurisprudência do Tribunal de Contas da União entende que a consulta de preços junto aos fornecedores não pode ser o único meio para obtenção de um valor de referência. Vejamos:

> As *pesquisas* de *preços* para aquisição de bens e contratação de serviços em geral devem ser baseadas em uma "cesta de *preços",* devendo-se dar preferência para *preços* praticados no âmbito da Administração Pública, oriundos de outros certames. A *pesquisa* de *preços* feita exclusivamente junto a fornecedores deve ser utilizada em último caso, na ausência de *preços* obtidos em contratações públicas anteriores ou cestas de *preços* referenciais (Instrução Normativa Seges-ME 73/2020). Acórdão 4958/2022-Primeira Câmara | Relator: AUGUSTO SHERMAN. (Grifamos)

A pesquisa de preços para elaboração do orçamento estimativo da licitação não deve se restringir a cotações realizadas junto a potenciais fornecedores, devendo ser utilizadas outras fontes como parâmetro, a exemplo de contratações públicas similares, sistemas referenciais de preços disponíveis, pesquisas na internet em sítios especializados e contratos anteriores do próprio órgão. Acórdão 713/2019-Plenário | Relator: BRUNO DANTAS. (Grifamos)

É essencial destacar que o preço de referência deve ser formado a partir de diversas fontes, dentre as quais os preços obtidos em licitações de outros órgãos públicos. O Art. 23 da Nova Lei de Licitações preceitua:

> Art. 23. O valor previamente estimado da contratação deverá ser compatível com os valores praticados pelo mercado, considerados os preços constantes de bancos de

> dados públicos e as quantidades a serem contratadas, observadas a potencial economia de escala e as peculiaridades do local de execução do objeto.
> § 1º No processo licitatório para aquisição de bens e contratação de serviços em geral, conforme regulamento, o valor estimado será definido com base no melhor preço aferido por meio da utilização dos seguintes parâmetros, adotados de forma combinada ou não:
> I - composição de custos unitários menores ou iguais à mediana do item correspondente no painel para consulta de preços ou no banco de preços em saúde disponíveis no Portal Nacional de Contratações Públicas (PNCP);
> II - contratações similares feitas pela Administração Pública, em execução ou concluídas no período de 1 (um) ano anterior à data da pesquisa de preços, inclusive mediante sistema de registro de preços, observado o índice de atualização de preços correspondente;
> III - utilização de dados de pesquisa publicada em mídia especializada, de tabela de referência formalmente aprovada pelo Poder Executivo federal e de sítios eletrônicos especializados ou de domínio amplo, desde que contenham a data e hora de acesso;
> IV - pesquisa direta com no mínimo 3 (três) fornecedores, mediante solicitação formal de cotação, desde que seja apresentada justificativa da escolha desses fornecedores e que não tenham sido obtidos os orçamentos com mais de 6 (seis) meses de antecedência da data de divulgação do edital;
> V - pesquisa na base nacional de notas fiscais eletrônicas, na forma de regulamento.

Em conformidade com o disposto na legislação foram realizadas pesquisas de preços de licitações realizadas no máximo há 12 meses por outros órgãos públicos nas plataformas Licitacon, Portal de Compras Públicas e Portal Nacional de Contratações Públicas (PNCP). No entanto, foi evidenciado que os processos disponíveis, embora sejam similares, apresentam elementos que não estão de acordo com as especificidades do objeto.

Nota-se que os valores das contratações são estabelecidos de acordo com cada contratante, considerando como elementos essências, para elaboração das propostas.

Verifica-se que o Consórcio Intermunicipal atualmente é composto por 25 (vinte e cinco) municípios consorciados, abrangendo uma população estimada em aproximadamente 496.000 (quatrocentos e noventa e seis mil) habitantes. Essa configuração revela uma realidade administrativa que diverge substancialmente dos modelos tradicionais de contratação por entes isolados, conforme se observa nas consultas realizadas em sítios eletrônicos especializados em compras e contratações públicas.

De modo geral, os processos licitatórios conduzidos de forma individual pelos municípios resultam em contratações de menor escala, o que naturalmente limita o número de fornecedores interessados e contratados. Já no âmbito da contratação compartilhada viabilizada pelo Consórcio, verifica-se a ampliação significativa do volume de serviços a serem executados, favorecendo a eficiência administrativa, a otimização dos recursos públicos e a ampliação do alcance das ações voltadas ao interesse coletivo.

Dessa forma, e em consonância com os princípios da economicidade, isonomia e seleção da proposta mais vantajosa, o Consórcio procedeu à realização de pesquisa de preços com, no mínimo, 3 (três) fornecedores distintos, mediante solicitação formal de cotação. Para a escolha dos fornecedores consultados, adotou-se como critério a experiência comprovada em procedimentos similares, bem como a capacidade técnico-operacional demonstrada, de modo a assegurar que a contratação pretendida atenda à complexidade e à abrangência exigidas pelo modelo consorciado.

Em observância à Instrução Normativa SEGES/ME Nº 65/2021, em seu Art 6º, foi utilizado como método para obtenção do preço estimado, a média dos preços obtidos na pesquisa de preços, cujo cálculo incide num conjunto frequentemente de no mínimo três preços, oriundos de vários parâmetros de que trata o art 5º, desconsiderando valores inexequíveis, inconsistente e excessivamente elevados.

14. DA JUSTIFICATIVA PARA ORÇAMENTO SIGILOSO

De acordo com a Lei 14.133/2021, art. 24 temos que “desde que justificado, o orçamento estimado da contratação **poderá ter caráter sigiloso**, sem prejuízo da divulgação do detalhamento dos quantitativos e das demais informações necessárias para a elaboração das propostas.” E desde que observado o que consta do inciso I e do Parágrafo único:

> I – o sigilo não prevalecerá para os órgãos de controle interno e externo;
> Parágrafo único. Na hipótese de licitação em que for adotado o critério de julgamento por maior desconto, o preço estimado ou o máximo aceitável constará do edital da licitação. (Grifamos.)

Assim, por se tratar de licitação na modalidade menor preço e pelo fato de a nova lei estabelecer um caráter discricionário para a decisão do caráter sigiloso ou não do orçamento, optaremos pela não divulgação do mesmo.

Entende-se, ainda, que a depender do mercado, a publicação do orçamento estimado da contratação ocasiona o chamado efeito âncora, elevando os preços das propostas o mais próximo possível do valor de referência da Administração. Nessas situações, a consagração de princípios próprios

da Administração Pública (interesse público e eficiência, sobretudo) recomendam que o preço orçado pela Administração seja mantido sob sigilo até o fim da disputa.

Nessa linha, Jorge Ulisses Jacoby Fernandes cita algumas das vantagens em se omitir o valor estimado (FERNANDES, 2009, p. 484-485):

> a) inibe a tentativa de a licitante limitar seu preço ao estimado na pesquisa;
> b) permite o Pregoeiro obter, na fase de lances e na negociação, preços inferiores aos da pesquisa;
> c) não vincula os preços à época da pesquisa, permitindo à equipe de apoio atualizá-los até no dia da própria sessão do pregão.

Conforme o exposto, e visando resguardar a regularidade, a competitividade e a obtenção da proposta mais vantajosa para a Administração, o CISGA adotará, como medida saneadora, a utilização do **orçamento sigiloso**, nos termos da Lei nº 14.133/2021.

A adoção dessa sistemática busca evitar que o valor estimado da contratação influencie a formulação das propostas pelos licitantes, estimulando a apresentação de preços efetivamente compatíveis com a realidade de mercado e promovendo maior competitividade entre os participantes.

Além disso, o orçamento sigiloso constitui mecanismo apto a preservar a economicidade da contratação, reduzindo o risco de alinhamento artificial de preços e assegurando que a disputa ocorra em condições de maior eficiência, sem prejuízo da transparência do procedimento, uma vez que o orçamento estimado será devidamente divulgado após o encerramento da fase de julgamento, em estrita observância à legislação aplicável.

15. DA JUSTIFICATIVA PARA A VEDAÇÃO À SUBCONTRATAÇÃO

O art. 122 da Lei n. 14.133, de 2021, admite a subcontratação parcial de obra, serviço ou fornecimento, até o limite autorizado pela Administração. A subcontratação, desde que autorizada pela Administração, possibilita que terceiro, que não participou do certame licitatório, realize parte do objeto.

Vejamos também a doutrina de Marçal Justen Filho:

> A subcontratação torna-se cabível, senão inevitável, quando o objeto licitado comporta uma execução complexa, em que algumas fases, etapas ou aspectos apresentam individualidade e são desempenhadas por terceiros especializados.
> A evolução dos princípios organizacionais produziu o fenômeno terceirização, que deriva dos princípios da especialização e da concentração de atividades. Em vez de

> desempenhar integralmente todos os ângulos de uma atividade, as empresas tornam-se especialistas em certos setores.
> A escolha da Administração deve ser orientada pelos princípios que regem a atividade privada.
> Na iniciativa privada, prevalece a subcontratação na execução de certas prestações. Essa é a solução economicamente mais eficiente e tecnicamente mais satisfatória.
> A Administração tem o dever de adotar as práticas mais eficientes, incorporando as práticas próprias da iniciativa privada. Logo, o ato convocatório deve permitir, quando viável, que idênticos procedimentos sejam adotados na execução do contrato administrativo.
> Ao admitir a subcontratação, a Administração obtém vantagens econômicas decorrentes dos ganhos de eficiência do particular contratado.
> Estabelecendo regras diversas das práticas entre os particulares, a Administração reduz a competitividade do certame. É óbvio que se pressupõe, em todas as hipóteses, que a Administração comprove se as práticas usuais adotadas pela iniciativa privada são adequadas para satisfazer os interesses fundamentais.
> A subcontratação pode representar inclusive um fator de ampliação da competição.
> Há certas atividades dotadas de especialização, complexidade e onerosidade diferenciada. Impor a sua execução de modo necessário pelo próprio contratado pode resultar na redução do universo de possíveis licitantes. Permitir a subcontratação em tais casos é justificado pelas mesmas razões que legitimam a participação de empresas em consórcio.
> (Comentários à lei de licitações e contratações administrativas. Thomson Reuters Revista dos Tribunais. Edição do Kindle. pp. 1349-1350).

O §2º do art. 122 possibilita que edital ou regulamento vedem, restrinjam ou estabeleçam condições para a subcontratação. Trata-se de uma faculdade. Portanto, não é obrigatório que o instrumento convocatório ou seus anexos estabeleçam limites à subcontratação.

No caso em questão, as características do certame, consubstanciado numa futura e eventual contratação de soluções de Adequação à Lei Geral de Proteção de Dados (LGPD), Serviços Gerenciados de Segurança Cibernética e Backup em Nuvem, denota não haver execução complexa, em que algumas fases, etapas ou aspectos apresentam individualidade. Por esses motivos, reputamos bem amparada a vedação ao expediente.

A administração, ao vedar a subcontratação, busca afastar o risco de descumprimento do contrato, sendo a execução integral, por parte das empresas contratadas, a maneira eficaz de garantir o controle técnico na prestação do serviço. As contratadas devem possuir todos os recursos necessários

para executar o objeto do contrato integralmente, não havendo componentes que precisem ser delegados a terceiros.

16. DA JUSTIFICATIVA PARA O NÃO PARCELAMENTO

A jurisprudência do TCU está pacificada no sentido de que a regra é que a adjudicação ocorra por item, sendo a adjudicação por lote a exceção, sendo necessário a justificativa da razão de sua necessidade. Essa questão está expressa na Súmula TCU 247:

> É obrigatória a admissão da adjudicação por item e não por preço global, nos editais das licitações para a contratação de obras, serviços, compras e alienações, cujo objeto seja divisível, desde que não haja prejuízo para o conjunto ou complexo ou perda de economia de escala, tendo em vista o objetivo de propiciar a ampla participação de licitantes que, embora não dispondo de capacidade para a execução, fornecimento ou aquisição da totalidade do objeto, possam fazê-lo com relação a itens ou unidades autônomas, devendo as exigências de habilitação adequar-se a essa divisibilidade.

Além disso, diversos Acórdãos também fixam essa linha de raciocínio:

> Em regra, as aquisições por parte de instituições públicas devem ocorrer por itens, sendo que no caso de opção de aquisição por lotes a composição destes deve ter justificativa plausível. TCU. Acórdão 2.077/2011, Plenário, Rel. Min. Augusto Sherman.
>
> O critério de julgamento de menor preço por lote somente deve ser adotado quando for demonstrada inviabilidade de se promover a adjudicação por item e evidenciadas razões que demonstrem ser aquele o critério que conduzirá a contratações economicamente mais vantajosas. Acórdão 1.680/2015, Plenário, Rel. Min. Marcos Bemquerer.

Diante disso, a regra sobre a forma de contratação nas licitações é por itens, sendo exceção a utilização do lote ou grupo, desde que haja necessidade técnica e econômica para tal agrupamento. No caso concreto do objeto do futuro certame, haverá o parcelamento da solução considerando a inviabilidade técnica e econômica para o não parcelamento.

Em conformidade com o disposto no art. 46 da Lei nº 14.133/2021, a Administração Pública deve, sempre que possível, promover o parcelamento do objeto da contratação, com vistas a ampliar a competitividade, fomentar a participação de um maior número de licitantes e propiciar a economicidade

do certame. Todavia, após análise técnica e econômica detida, verifica-se que, no presente caso, o parcelamento da contratação se mostra inviável e inconveniente à Administração Pública, seja sob o ponto de vista técnico-operacional, seja sob o aspecto da gestão contratual e financeira.

Trata-se, portanto, de uma solução técnica estruturalmente indivisível, composta por um ciclo de atividades dependentes e que exigem plena integração entre os recursos humanos, os insumos e os equipamentos já disponibilizados pela Administração consorciada. A fragmentação do objeto comprometeria a padronização dos procedimentos, aumentaria o risco de inconsistências operacionais, dificultaria a fiscalização e tornaria a gestão contratual mais onerosa e ineficiente.

Diante do exposto, conclui-se que o parcelamento da solução não atenderia aos princípios da que norteiam as contratações desta Administração, podendo ainda comprometer a qualidade técnica da execução contratual e o atingimento dos resultados pretendidos.

17. DA JUSTIFICATIVA PARA NÃO EXIGÊNCIA DE GARANTIA DA EXECUÇÃO

A Nova Lei de Licitações estabelece:

> Art. 96. A critério da autoridade competente, em cada caso, poderá ser exigida, mediante previsão no edital, prestação de garantia nas contratações de obras, serviços e fornecimentos.
> § 1º Caberá ao contratado optar por uma das seguintes modalidades de garantia:
> I - caução em dinheiro ou em títulos da dívida pública emitidos sob a forma escritural, mediante registro em sistema centralizado de liquidação e de custódia autorizado pelo Banco Central do Brasil, e avaliados por seus valores econômicos, conforme definido pelo Ministério da Economia;
> II - seguro-garantia;
> III - fiança bancária emitida por banco ou instituição financeira devidamente autorizada a operar no País pelo Banco Central do Brasil.
> IV - título de capitalização custeado por pagamento único, com resgate pelo valor total. (Incluído pela Lei nº 14.770, de 2023)
> § 2º Na hipótese de suspensão do contrato por ordem ou inadimplemento da Administração, o contratado ficará desobrigado de renovar a garantia ou de endossar a apólice de seguro até a ordem de reinício da execução ou o adimplemento pela Administração.
> § 3º O edital fixará prazo mínimo de 1 (um) mês, contado da data de homologação da licitação e anterior à assinatura do contrato, para a prestação da garantia pelo contratado quando optar pela modalidade prevista no inciso II do § 1º deste artigo.

Art. 97. O seguro-garantia tem por objetivo garantir o fiel cumprimento das obrigações assumidas pelo contratado perante à Administração, inclusive as multas, os prejuízos e as indenizações decorrentes de inadimplemento, observadas as seguintes regras nas contratações regidas por esta Lei:

I - o prazo de vigência da apólice será igual ou superior ao prazo estabelecido no contrato principal e deverá acompanhar as modificações referentes à vigência deste mediante a emissão do respectivo endosso pela seguradora;

II - o seguro-garantia continuará em vigor mesmo se o contratado não tiver pago o prêmio nas datas convencionadas.

Parágrafo único. Nos contratos de execução continuada ou de fornecimento contínuo de bens e serviços, será permitida a substituição da apólice de seguro-garantia na data de renovação ou de aniversário, desde que mantidas as mesmas condições e coberturas da apólice vigente e desde que nenhum período fique descoberto, ressalvado o disposto no § 2º do art. 96 desta Lei.

Art. 98. Nas contratações de obras, serviços e fornecimentos, a garantia poderá ser de até 5% (cinco por cento) do valor inicial do contrato, autorizada a majoração desse percentual para até 10% (dez por cento), desde que justificada mediante análise da complexidade técnica e dos riscos envolvidos.

Parágrafo único. Nas contratações de serviços e fornecimentos contínuos com vigência superior a 1 (um) ano, assim como nas subsequentes prorrogações, será utilizado o valor anual do contrato para definição e aplicação dos percentuais previstos no caput deste artigo.

Art. 99. Nas contratações de obras e serviços de engenharia de grande vulto, poderá ser exigida a prestação de garantia, na modalidade seguro-garantia, com cláusula de retomada prevista no art. 102 desta Lei, em percentual equivalente a até 30% (trinta por cento) do valor inicial do contrato.

Art. 100. A garantia prestada pelo contratado será liberada ou restituída após a fiel execução do contrato ou após a sua extinção por culpa exclusiva da Administração e, quando em dinheiro, atualizada monetariamente.

Art. 101. Nos casos de contratos que impliquem a entrega de bens pela Administração, dos quais o contratado ficará depositário, o valor desses bens deverá ser acrescido ao valor da garantia.

Desse modo, conforme observa-se do artigo acima descrito, a garantia contratual somente será exigida quando a complexidade do valor da contratação importar em consideráveis riscos de prejuízos à Administração em razão do inadimplemento do contratado. Não por acaso, também é o parâmetro aventado pelo TCU, segundo o qual a garantia deve ser exigida nas contratações de maior valor, envolvendo alta

> complexidade técnica e riscos financeiros consideráveis (Acórdão n. 3.126/2012 – Plenário).

Vejamos o alerta de Marçal Justen Filho:

> "A Lei remete à discricionariedade da Administração a exigência da garantia. Poderá (deverá) ser exigida apenas nas hipóteses em que se faça necessária. Quando inexistirem riscos de lesão ao interesse estatal, a Administração não precisará impor a prestação de garantia." (Comentários à Lei de Licitações e Contratos Administrativos, 11ª ed., São Paulo: Dialética, 2005, p. 499).

Assim, a exigência deve ser avaliada em cada caso concreto, com base no grau de risco de prejuízo ao interesse público, frente à particularidade do objeto licitado. Nessa senda, cabe destacar que o objeto deste visa a futura e eventual contratação de soluções de Adequação à Lei Geral de Proteção de Dados (LGPD), Serviços Gerenciados de Segurança Cibernética e Backup em Nuvem, denota não haver execução complexa, em que algumas fases, etapas ou aspectos apresentam riscos. Portanto, é possível concluir pela inexistência de riscos consideráveis à Administração que importem na exigência de uma garantia contratual.

Destarte, considera-se justificada a não exigência de garantia.

18. DA JUSTIFICATIVA PARA INADMISSÃO DE CONSÓRCIOS

A Lei nº 14.133/2021 tem como regra a permissão à participação de consórcios, inclusive quando o instrumento for omisso sobre o tema. A Administração Pública, quando não permitir a participação de licitantes em consórcios, deve motivar essa decisão, justificando as razões para tanto.

O ato convocatório poderá admitir ou não a participação de consórcio, sendo essa decisão resultado de um processo de avaliação da realidade do mercado em razão do objeto a ser licitado e da ponderação dos riscos inerentes à atuação de uma pluralidade de sujeitos associados para execução do objeto visando ao atendimento do interesse público. Logicamente, trata-se de escolha que consubstancia um ato discricionário da Administração Pública o rechaço editalício a essas formações empresariais, o que evidentemente não significa autorização para decisões arbitrárias ou imotivadas. Por este motivo, a Autoridade Licitante, dentro do poder discricionário de melhor conveniência e oportunidade decidirá pela vedação ou não à participação de empresas em regime de consórcio.

Nessa senda, veja-se que a jurisprudência do TCU era pacífica com relação ao poder discricionário da Administração para admitir ou não a participação de empresas em consórcio, nos termos do art. 33 da revogada Lei 8.666/1993. Leia-se o Informativo nº 106, do TCU:

> PLENÁRIO Fica ao juízo discricionário da Administração pública a decisão, devidamente motivada, quanto à possibilidade de participação ou não em licitações de empresas em consórcio Relatório de Auditoria do Tribunal tratou das obras do Projeto de Integração do Rio São Francisco com as bacias hidrográficas do Nordeste Setentrional (PISF), especificamente do Lote 5, do Edital de Concorrência nº 12011/2011, realizada pelo Ministério da Integração Nacional – (MI). Uma das irregularidades apontadas foi a restrição à participação de empresas em consórcio. Segundo o MI, "a participação de empresas sob a forma de consórcio envolveria a discricionariedade da Administração", sendo que, conforme precedente jurisprudencial do TCU, "o juízo acerca da admissão ou não de empresas consorciadas na licitação dependerá de cada caso concreto". Ao concordar com a alegação apresentada, o relator registrou em seu voto que "há que se demonstrar com fundamentos sólidos a escolha a ser feita pelo gestor durante o processo de licitação no que toca à vedação da participação de consórcios, ou mesmo à sua autorização". Deveria ser analisada, portanto, a situação de cada empreendimento, a partir de suas variáveis, tais quais o risco à competitividade, as dificuldades de gestão da obra e a capacitação técnica dos participantes. Diante disso, a partir do que fora examinado pela unidade instrutiva, para o relator, "**há que se ponderar para o fato de que cabe ao gestor definir qual o caminho a tomar relativamente à participação ou não de consórcios, de forma motivada no âmbito do processo licitatório**". Nos termos do voto do relator, o Plenário manifestou sua anuência. Precedente citado: Acórdão nº 1246/2006, do Plenário. Acórdão n.º 1165/2012-Plenário, TC 037.773/2011-9, rel. Min. Raimundo Carreiro, 16.5.2012. (grifamos)

De observar, contudo, que, mesmo com a mudança promovida com a edição da NLLCA, a doutrina segue afirmando que a vedação à participação dessas associações empresariais continua sendo uma decisão discricionária do administrador público, como alude, por exemplo, o escólio de Ronny Charles, já proferido sob a égide da Lei nº 14.133/2021[2]:

> O legislador não criou regra expressa acerca da obrigatoriedade ou não da participação dos consórcios. Essa decisão ficará a cargo do administrador, de acordo com regras de boa gestão que objetivem a ampliação da competitividade.

[2] CHARLES, Ronny. Leis de Licitações Públicas Comentadas. São Paulo: Editora Juspodivm, 2022, p. 138.

O grande norte a ser levado em conta para subsidiar o posicionamento administrativo é uma das grandes razões de ser do processo licitatório: a ampliação da competitividade. Com efeito, só será concebida a franquia à presença de tais formações empresariais quando isso representar estímulo ou acréscimo ao caráter competitivo do certame. Tais nuances são muito bem delineadas pela doutrina sempre precisa de Marçal Justen Filho[3]:

> "Em regra, o consórcio não é favorecido ou incentivado pelo nosso Direito. Como instrumento de atuação empresarial, o consórcio pode conduzir a resultados indesejáveis. A formação de consórcios acarreta riscos da dominação do mercado, através de pactos de eliminação de competição entre empresários. No campo de licitações, a formação de consórcios poderia reduzir o universo da disputa. O consórcio poderia retratar uma composição entre eventuais interessados, em vez de estabelecerem disputa entre si, formalizariam acordo para eliminar a competição.
>
> Mas o consórcio também pode prestar-se a resultados positivos e compatíveis com a ordem jurídica. Há hipóteses em que as circunstâncias de mercado e (ou) a complexidade do objeto tornam problemática a competição. Isso se passa quando grande quantidade de empresas, isoladamente, não dispuserem de condições para participar de licitações. Nesse caso, o instituto do é a via adequada para propiciar a ampliação do universo de participantes.
>
> É usual que a Administração Pública apenas autorize a participação de empresas em consórcio quando as dimensões ou a complexidade do objeto ou as circunstâncias concretas exijam a associação entre particulares. São as hipóteses em que apenas umas poucas empresas estariam aptas a preencher as condições especiais exigidas para a licitação".

Assim, nota-se que critérios como as circunstâncias do mercado ou a complexidade do objeto são os termômetros a indicar se a participação dos consórcios realizará o único objetivo legítimo encontrado na permissão: a ampliação da competitividade. Por suposto, casos há em que a franquia não possibilitará o alcance dessa nobre finalidade, acabando por produzir resultado diametralmente oposto. A decisão administrativa, nesse sentido, reveste-se, em linguagem coloquial, de caráter de "faca de dois gumes". A doutrina trata de aclarar essa conjuntura: "*Portanto, sempre que o objeto licitado for marcadamente vultuoso ou de composição complexa e inomogênea, o ente licitante deverá*

[3] FILHO, Marçal Justen. Comentários à Lei de Licitações e Contratos Administrativos. São Paulo: Dialética, 2009, p. 47.

obrigatoriamente admitir a participação de coligações empresárias no certame. Em outras palavras, tem-se que o ordenamento jurídico brasileiro e o seu conjunto de princípios informadores impõem a admissão de consórcios em grandes ou heteróclitas licitações – sob pena de restar asfixiado o princípio da competitividade e, em algumas circunstâncias, a própria licitação acabar convertida em procedimento inidôneo e ineficaz"[4]. A jurisprudência do TCU, de sua vez, confirma exatamente que os critérios enunciados pela lição doutrinária são os móveis a balizarem a decisão administrativa acerca dos consórcios, sempre na busca da preservação da competitividade:

> A jurisprudência deste Tribunal já se firmou no sentido de que a admissão ou não de consórcio de empresas em licitações e contratações é competência discricionária do administrador, devendo este exercê-la sempre mediante justificativa fundamentada. Não obstante a participação de consórcio seja recomendada sempre que o objeto seja considerado de alta complexidade ou vulto, tal alternativa também não é obrigatória. **Devem ser consideradas as circunstâncias concretas que indiquem se o objeto apresenta vulto ou complexidade que torne restrito o universo de possíveis licitantes. Somente nessa hipótese, fica o administrador obrigado a autorizar a participação de consórcio de empresas no certame, com o intuito precípuo de ampliar a competitividade e proporcionar a obtenção da proposta mais vantajosa.** (TCU, Acórdão 2.831, Plenário, Rel. Min. Ana Arraes). (Grifo nosso)

É bem importante, por essas veredas, pontuar que o contrário é absolutamente verdadeiro. A chancela à presença de consórcios poderá ocasionar uma restrição à competitividade, haja vista que reduz a probabilidade de que sociedade empresárias mais modestas, de maneira isolada, venham a ser vencedoras nas licitações, à míngua de fundamento legal para tanto. Nesse sentido, é extremamente elucidativa a decisão proferida pelo TCE/MG no Recurso Ordinário n. 997720:

> (...) consoante jurisprudência do Tribunal de Contas da União, "a participação de consórcio é recomendada sempre que o objeto seja considerado de alta complexidade ou vulto". (Acórdão nº 2831/2012 – TCU – Plenário)

[4] RIBEIRO, João Paulo da Silveira; TEIXEIRA, João Pedro Accioly. A participação de consórcios empresariais em procedimentos licitatórios: Livre escolha da Administração licitante? Brasília: Revista do TCU, Setembro/Dezembro 2015.

Em outras palavras, a autorização para a participação de empresas em consórcio afigura-se como regra quando a licitação apresentar **vulto ou complexidade que torne restrito o universo de possíveis licitantes**, nos seguintes termos:

> *(...) 2. A jurisprudência deste Tribunal já se firmou no sentido de que a admissão ou não de consórcio de empresas em licitações e contratações é competência discricionária do administrador, devendo este exercê-la sempre mediante justificativa fundamentada.*
> *3. Não obstante a participação de consórcio seja recomendada sempre que o objeto seja considerado de alta complexidade ou vulto, tal alternativa também não é obrigatória.*
> 4. Devem ser consideradas as circunstâncias concretas que indiquem se o objeto apresenta vulto ou complexidade que torne restrito o universo de possíveis licitantes. Somente nessa hipótese, fica o administrador obrigado a autorizar a participação de consórcio de empresas no certame, com o intuito precípuo de ampliar a competitividade e proporcionar a obtenção da proposta mais vantajosa. (Acórdão 2831/2012 – Plenário- TCU) (grifo nosso)
> Ainda nesse sentido, cabe citar novamente a decisão do Tribunal de Contas da União aprovada em Plenário, de relatoria do Ministro Marcos Bemquerer (Acórdão nº 1946/2006).

Quando o objeto a ser licitado envolve questões de alta complexidade, via de regra, a Administração, com o intuito de aumentar o número de participantes, admite a formação de consórcio. Assim, em licitações complexas, a lógica é que a participação de empresas em consórcio, como regra, seja ampliativa da competitividade, razão pela qual a vedação, por certo, deverá ser justificada.

Compreendido esse ponto, necessário trazer à baila o outro lado da moeda, qual seja o critério a ser utilizado quando se trata da licitação comum, de menor monta, vulto ou complexidade, até porque tal situação não é comumente abordada nem na doutrina, nem na jurisprudência.

Neste caso, como argumento integrativo, pertinente utilizar o denominado raciocínio contrário sensu, nos seguintes termos: se nas licitações complexas, o pressuposto é de que a participação de empresas em consórcio amplia a competitividade, em licitações comuns a lógica se inverte e o pressuposto é de que a admissão de consórcios pode levar à restrição da competitividade, uma vez que retira ou reduz a possibilidade de que empresas menores, isoladamente, possam sagrar-se vencedoras nas licitações, sem que haja fundamento para tanto.

Dessarte, a sistemática que ora se propõe como fator condicionante da limitação ao poder discricionário da Administração Pública pode ser assim sistematizada: (1) naquelas licitações em que o objeto for comum, simples e de pequena monta, a vedação impõe-se como regra, posto que os consórcios, em tese, restringem a competitividade e lado outro, (2) nos certames de grande vulto e complexidade, o raciocínio se inverte e a regra geral passa a ser a permissão dos consórcios. Nessa situação, a título exemplificativo, sinaliza-se (apenas) como um indicativo, sua ocorrência especialmente em licitações na modalidade Concorrência, cuja lógica, até pelos valores dos objetos licitados, aponta para um maior vulto, dimensão e grau de complexidade do objeto licitado.

Portanto, a melhor conduta a ser adotada pelo gestor público é a de avaliar as condições objetivas da contratação, os requisitos técnicos e econômicos envolvidos e, bem sopesados, optar por permitir, ou não, a participação de empresas reunidas em consórcio.

Em síntese, fica por último um alerta. O que deve ser observado é que a participação de empresas em consórcio na licitação deve ter como parâmetro a conjugação de elementos como vulto, dimensão e complexidade, não querendo significar, por exemplo, que somente o valor de uma licitação é suficiente para caracterizar a exigência de participação/vedação em consórcio. Repita-se então que tal aferição deve levar em conta também a natureza do objeto.

Com relação à presente contratação, a vedação à participação de interessadas que se apresentem constituídas sob a forma de consórcio se justifica para que ocorra a devida garantia de disputa, à medida em que, caso contrário, a presença de tais associação empresariais acabariam por reduzir a possibilidade de sociedades empresárias isoladas ou menores serem escolhidas ao final do torneio.

Em derradeiro, avaliando a realidade do mercado que pode ser medida através da ampla participação, em todos certames promovidos pelo CISGA desde 2013, de uma vasta gama de sociedades empresárias não organizadas sob o arranjo consorcial, não se mostra necessária a participação dessa espécie empresarial, a qual poderá ainda se mostrar contraproducente em relação a sua principal finalidade: a ampliação da disputa. Em conclusão, dessarte, entendemos amplamente fundamentada a vedação aos consórcios.

19. DO GERENCIAMENTO DE RISCOS

Risco	Probabilidade	Impacto	Mitigação
Não aprovação dos parâmetros previstos no Termo de Referência	Média	Alto	Revisar os documentos primários, como o estudo preliminar, com o objetivo de mitigar possíveis divergências legais e técnicas para a realização do processo licitatório. Necessário conhecimento de

Risco	Probabilidade	Impacto	Mitigação
			procedimentos e legislação para elaboração do Termo de Referência.
Contratar fornecedor que não tenha expertise comprovada	Média	Alto	Realizar uma análise criteriosa de mercado e verificar as qualificações técnicas e experiências do fornecedor.
Atraso na implantação da solução	Baixa	Médio	Estabelecer cronograma detalhado com marcos e penalidades para atrasos.
Baixa adesão dos servidores aos processos de adequação à LGPD.	Média	Médio	Promover campanhas de sensibilização e treinamentos sobre a LGPD.
Não conformidade com a Lei 14.133/2021	Baixa	Alto	Incluir cláusulas específicas de conformidade legal no contrato e realizar auditorias periódicas.
Indisponibilidade dos serviços e equipamentos contratados	Média	Alto	Exigir SLA (Service Level Agreement) com tempos de resposta e resolução adequados, incluindo substituição de equipamentos em caso de falha.
Demandas imprevistas durante a execução contratual	Média	Médio	Utilizar as horas técnicas contratadas para atendimento de demandas extraordinárias, devidamente dimensionadas com base no diagnóstico prévio.
Vazamento de dados sensíveis	Baixa	Alto	Realizar treinamentos e campanhas de sensibilização com os servidores sobre o tratamento adequado de dados pessoais classificados como sensíveis.
Resistência à mudança por parte dos servidores	Média	Médio	Promover campanhas de sensibilização para os servidores, destacando a importância da proteção de dados e os benefícios da solução, bem como treinamentos sobre a LGPD e Segurança da Informação.
Mudanças na legislação	Baixa	Médio	Incluir cláusulas de adaptação a novas leis e regulamentos.
Problemas de suporte técnico	Média	Médio	Avaliar histórico de suporte do fornecedor e definir pontos de contato claros.
Falta de uso pleno da solução contratada	Média	Médio	Monitorar a utilização da solução e fornecer relatórios de desempenho aos gestores municipais.

20. DAS PROVIDÊNCIAS PRÉVIAS AO CONTRATO

Previamente à celebração dos contratos, os contratantes deverão providenciar a capacitação dos servidores para fiscalização e gestão contratual, bem como implementar/ manter sistemas e rotinas de acompanhamento e controle.

21. DAS CONTRATAÇÕES CORRELATAS/INTERDEPENDENTES

Não há contratações correlatas ou interdependentes.

22. DOS POSSÍVEIS IMPACTOS AMBIENTAIS E CRITÉRIOS DE SUSTENTABILIDADE

Considerando a natureza do objeto da contratação, não se identificam impactos ambientais significativos decorrentes de sua execução. Todavia, a futura contratada deverá observar e cumprir os critérios e as diretrizes de sustentabilidade ambiental estabelecidos na Seção 6 deste Estudo Técnico Preliminar, adotando práticas compatíveis com a legislação vigente e com os princípios da sustentabilidade aplicáveis à contratação.

23. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

Considerando a natureza do Sistema de Registro de Preços e a possibilidade de que outros órgãos e entidades da Administração Pública apresentem necessidade futura de contratação dos mesmos objetos, mostra-se conveniente permitir a adesão à Ata de Registro de Preços por órgãos e entidades que não tenham participado dos procedimentos iniciais da licitação, desde que observadas as condições e os limites estabelecidos no instrumento convocatório e na legislação aplicável.

A possibilidade de adesão contribui para o aproveitamento da economia de escala obtida no procedimento licitatório, evitando a realização de novos processos administrativos para contratação de objetos já submetidos à disputa e cujos preços foram registrados. A medida também favorece a racionalização dos recursos públicos, a redução dos custos administrativos e a maior eficiência das contratações públicas.

A utilização da Ata por órgãos não participantes ficará condicionada à prévia consulta e aceitação do Órgão Gerenciador, bem como à concordância do fornecedor beneficiário do registro, assegurando-se, em cada caso, a análise da compatibilidade da adesão com as condições originalmente estabelecidas e a capacidade de atendimento da demanda.

A adesão deverá, ainda, ser precedida de justificativa quanto à vantagem da utilização da Ata, de modo a demonstrar que a contratação por meio do registro de preços se mostra adequada e vantajosa para o órgão ou entidade não participante, considerando as condições de mercado e as características do objeto.

Com o objetivo de preservar o equilíbrio da Ata e evitar que as adesões comprometam o atendimento dos órgãos gerenciador e participantes, serão observados os limites quantitativos estabelecidos no edital, de modo que as aquisições ou contratações adicionais por órgão ou entidade não participante não poderão exceder, individualmente, 50% (cinquenta por cento) dos quantitativos dos itens registrados para o órgão gerenciador e os órgãos participantes.

Da mesma forma, o quantitativo total decorrente das adesões não poderá exceder, na sua totalidade, 200% (duzentos por cento) do quantitativo de cada item registrado para o órgão gerenciador e os órgãos participantes, independentemente do número de órgãos ou entidades não participantes que venham a aderir à Ata.

Dessa forma, a previsão de adesão mostra-se tecnicamente e administrativamente conveniente, pois amplia o potencial de utilização dos resultados do procedimento licitatório, promove maior eficiência e economicidade nas contratações públicas e possibilita o atendimento de demandas de outros órgãos e entidades, sem afastar os mecanismos de controle, os limites quantitativos e as condições necessárias à preservação da segurança e do equilíbrio da Ata de Registro de Preços.

24. DOS RESULTADOS PRETENDIDOS

A presente contratação tem por objetivo viabilizar a implementação efetiva dos princípios, diretrizes e requisitos estabelecidos pela Lei Geral de Proteção de Dados Pessoais (LGPD), por meio da disponibilização de uma solução tecnológica integrada e de suporte técnico especializado, capazes de proporcionar à Administração Pública instrumentos adequados para o gerenciamento da privacidade e da segurança da informação. A solução permitirá o mapeamento dos processos administrativos, o inventário dos dados pessoais tratados, a identificação, análise, avaliação e tratamento dos riscos relacionados ao tratamento dessas informações, bem como a definição, implementação e acompanhamento de planos de ação destinados à adoção dos controles necessários para a conformidade com a legislação vigente.

A realização desse diagnóstico permitirá identificar vulnerabilidades existentes nos processos internos, classificando-as de acordo com seu grau de criticidade, o que possibilitará aos gestores públicos estabelecer prioridades na implantação de medidas corretivas e preventivas, direcionando os recursos disponíveis de forma mais eficiente e alinhada ao interesse público.

A contratação também possibilitará que todas as situações identificadas sejam analisadas sob uma perspectiva multidisciplinar, contemplando aspectos jurídicos, tecnológicos e de gestão de processos, assegurando que as medidas adotadas sejam suficientes para promover a adequada conformidade à LGPD e fortalecer a governança da informação no âmbito da Administração Pública.

Além disso, o levantamento dos processos organizacionais, o inventário dos dados pessoais e o gerenciamento dos riscos deverão possibilitar a geração automatizada do Relatório de Impacto à Proteção de Dados Pessoais (RIPD), documento essencial para demonstrar a conformidade das atividades de tratamento de dados e subsidiar a tomada de decisões relacionadas à proteção da privacidade dos titulares.

A contratação contempla, ainda, a prestação de suporte técnico especializado durante toda a execução contratual, abrangendo a capacitação dos usuários, o treinamento das equipes responsáveis e o acompanhamento da utilização da plataforma, garantindo que gestores e servidores públicos estejam aptos a utilizar adequadamente a ferramenta e a aplicar, na prática, os princípios e fundamentos previstos na Lei Geral de Proteção de Dado.

Cumpre destacar que a LGPD impõe aos órgãos públicos o dever de adotar medidas técnicas e administrativas aptas a proteger os dados pessoais sob sua responsabilidade, assegurando a privacidade dos cidadãos e reduzindo os riscos decorrentes de incidentes de segurança da informação. Considerando que os diversos setores da Administração tratam diariamente elevado volume de dados pessoais e informações sensíveis, abrangendo áreas como saúde, educação, assistência social, recursos humanos, administração tributária e gestão interna, torna-se imprescindível a adoção de mecanismos capazes de garantir a confidencialidade, a integridade e a disponibilidade dessas informações, prevenindo acessos indevidos, vazamentos, perdas de dados e demais eventos que possam comprometer a continuidade e a confiabilidade dos serviços públicos.

Nesse contexto, a implementação de mecanismos de monitoramento contínuo da infraestrutura tecnológica, incluindo soluções de gerenciamento e correlação de eventos de segurança (SIEM) e Centro de Operações de Segurança (SOC), permitirá à Administração identificar, monitorar e responder de forma proativa a incidentes de segurança cibernética, reduzindo significativamente os riscos operacionais e assegurando maior estabilidade, disponibilidade e confiabilidade dos sistemas utilizados pelos municípios consorciados. O monitoramento permanente também possibilitará a identificação tempestiva de vulnerabilidades, permitindo a adoção de medidas preventivas antes que estas sejam exploradas por agentes maliciosos, fortalecendo a resiliência da infraestrutura tecnológica.

Por fim, a contratação de empresa especializada garantirá à Administração o acesso contínuo a profissionais com conhecimento técnico qualificado nas áreas de proteção de dados, segurança da informação e governança digital, proporcionando suporte especializado para a implementação das melhores práticas de mercado, atualização constante dos controles de segurança e atendimento às exigências legais e regulatórias. Dessa forma, a contratação contribuirá para a consolidação de uma cultura institucional voltada à proteção de dados pessoais, à segurança da informação e ao

aprimoramento da governança pública, promovendo maior eficiência administrativa, redução de riscos e fortalecimento da confiança dos cidadãos nos serviços prestados pela Administração.

25. CONCLUSÕES SOBRE A VIABILIDADE DA CONTRATAÇÃO

Diante do exposto, conclui-se pela viabilidade de contratação por meio do Pregão Eletrônico para Registo de Preço, com atendimento à legislação aplicável, para atendimento das demandas do consórcio, e com benefícios evidentes para os municípios consorciados.

Garibaldi, 17 de setembro de 2026.

RUDIMAR CABERLON:47751517034
Assinado de forma digital por RUDIMAR CABERLON:47751517034
Dados: 2026.09.17 16:24:42 -03'00'

RUDIMAR CABERLON
Diretor Executivo CISGA

Aprovo o presente Estudo Técnico Preliminar.

NELTON CARLOS CONTE:53096797072
Assinado de forma digital por NELTON CARLOS CONTE:53096797072
Dados: 2026.09.17 16:43:54 -03'00'

NELTON CARLOS CONTE
Presidente Consórcio Intermunicipal de Desenvolvimento Sustentável da Serra Gaúcha CISGA