

PREGÃO ELETRÔNICO

mnbv

CONTRATANTE (UASG)

INSTITUTO FEDERAL DE SANTA CATARINA (158516)

OBJETO

AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TECNOLOGIA DA INFORMAÇÃO PARA O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA.

VALOR TOTAL DA CONTRATAÇÃO

R\$ 10.646.626,12

DATA DA SESSÃO PÚBLICA

Dia 26/03/2024 às 09h00min (horário de Brasília)

CRITÉRIO DE JULGAMENTO:

menor preço por item

MODO DE DISPUTA:

aberto e fechado

PREFERÊNCIA ME/EPP/EQUIPARADAS

SIM



Baixe o APP Compras.gov.br
e apresente sua proposta!

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA - IFSC

PREGÃO ELETRÔNICO Nº 31009/2023

(Processo Administrativo nº 23292.034402/2023-70)

Torna-se público que o(a) Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, por meio do Departamento de Compras, sediado à rua 14 de Julho, 150, Coqueiros, CEP:88075-010, Florianópolis-SC, realizará licitação, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da [Lei nº 14.133, de 2021](#), e demais legislação aplicável e, ainda, de acordo com as condições estabelecidas neste Edital.

1. DO OBJETO

- 1.1. O objeto da presente licitação é a contratação de solução de segurança em tecnologia da informação e comunicação composta por *appliances* de *backup*, *firewalls*, equipamentos de conexão de rede de dados (com/sem fio), conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.
- 1.2. A licitação será dividida em grupos e itens, conforme tabela constante do Termo de Referência, facultando-se ao licitante a participação em quantos grupos/itens forem de seu interesse.
 - 1.2.1. Itens não associados - 3 itens;
 - 1.2.2. Grupo 1 - Rede sem fio - 8 itens;
 - 1.2.3. Grupo 2 - Conexão de Rede - 8 itens;
 - 1.2.4. Grupo 3 - Segurança de Rede - 17 itens
 - 1.2.5. Grupo 4 - Backup de Dados -2 itens

2. DO REGISTRO DE PREÇOS

- 2.1. As regras referentes aos órgãos gerenciador e participantes, bem como a eventuais adesões são as que constam no Termo de Referência e na minuta de Ata de Registro de Preços.

3. DA PARTICIPAÇÃO NA LICITAÇÃO

- 3.1. Poderão participar deste Pregão os interessados que estiverem previamente credenciados no Sistema de Cadastramento Unificado de Fornecedores - SICAF e no Sistema de Compras do Governo Federal (www.gov.br/compras).
- 3.2. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 3.3. 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.
- 3.4. 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.
- 3.5. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação.
- 3.6. Para os itens 01 e 49, a participação é exclusiva a microempresas e empresas de pequeno porte, nos termos do [art. 48 da Lei Complementar nº 123, de 14 de dezembro de 2006](#).
- 3.6.1. 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. Para todos os itens, com exceção dos itens 1 e 49, a participação é restrita a empresas que cumpram o Processo Produtivo Básico nos termos das Leis nº 8.248, de 23 de outubro de 1991, e 8.387, de 30 de dezembro de 1991.
- 3.8. Será concedido tratamento favorecido para as microempresas e empresas de pequeno porte, para o microempreendedor individual - MEI, nos limites previstos da [Lei Complementar nº 123, de 2006](#) e do Decreto n.º 8.538, de 2015, bem como para bens e serviços produzidos com tecnologia produzida no país e bens produzidos de acordo com processo produtivo básico, na forma do art. 3º da Lei nº 8.248, de 1991 e art. 8º do Decreto nº 7.174, de 2010.
- 3.9. Não poderão disputar esta licitação:
- 3.9.1. aquele que não atenda às condições deste Edital e seu(s) anexo(s);
- 3.9.2. 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;
- 3.9.3. 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;
- 3.9.4. pessoa física ou jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;
- 3.9.5. 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

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau;

- 3.9.6. empresas controladoras, controladas ou coligadas, nos termos da Lei nº 6.404, de 15 de dezembro de 1976, concorrendo entre si;
- 3.9.7. 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;
- 3.9.8. agente público do órgão ou entidade licitante;
- 3.9.9. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;
- 3.9.10. 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 3.9.4 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 3.9.2 e 3.9.3 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 3.9.2 e 3.9.3 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 3.9.8 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. DA APRESENTAÇÃO DA PROPOSTA E DOS DOCUMENTOS DE HABILITAÇÃO

- 4.1. Na presente licitação, a fase de habilitação sucederá as fases de apresentação de propostas e lances e de julgamento.
- 4.2. Os licitantes encaminharão, exclusivamente por meio do sistema eletrônico, a proposta com 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.
- 4.3. Caso a fase de habilitação anteceda as fases de apresentação de propostas e lances, os licitantes encaminharão, na forma e no prazo estabelecidos no item anterior, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto nos itens 8.1.1 e 8.13.1 deste Edital.
- 4.4. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:
 - 4.4.1. está ciente e concorda com as condições contidas no edital e seus anexos, bem como de que a proposta apresentada 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 sua entrega em definitivo e que cumpre plenamente os requisitos de habilitação definidos no instrumento convocatório;
 - 4.4.2. não emprega menor de 18 anos em trabalho noturno, perigoso ou insalubre e não emprega menor de 16 anos, salvo menor, a partir de 14 anos, na condição de aprendiz, nos termos do [artigo 7º, XXXIII, da Constituição](#);
 - 4.4.3. 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](#);
 - 4.4.4. 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.
- 4.5. O licitante organizado em cooperativa deverá declarar, ainda, em campo próprio do sistema eletrônico, que cumpre os requisitos estabelecidos no [artigo 16 da Lei nº 14.133, de 2021](#).
- 4.6. 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 3º 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 nº 14.133, de 2021](#).
 - 4.6.1. no item exclusivo para participação de microempresas e empresas de pequeno porte, a assinalação do campo “não” impedirá o prosseguimento no certame, para aquele item;
 - 4.6.2. nos itens em que a participação não for exclusiva para microempresas e empresas de pequeno porte, a assinalação do campo “não” apenas produzirá o efeito de o licitante não ter direito ao tratamento favorecido previsto na [Lei Complementar nº 123, de 2006](#), mesmo que microempresa, empresa de pequeno porte ou sociedade cooperativa.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 4.7. A falsidade da declaração de que trata os itens 4.4 ou 4.6 sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e neste Edital.
- 4.8. Os licitantes poderão retirar ou substituir a proposta ou, na hipótese de a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, os documentos de habilitação anteriormente inseridos no sistema, até a abertura da sessão pública.
- 4.9. Não haverá ordem de classificação na etapa de apresentação da proposta e dos documentos de habilitação pelo licitante, o que ocorrerá somente após os procedimentos de abertura da sessão pública e da fase de envio de lances.
- 4.10. Serão disponibilizados para acesso público os documentos que compõem a proposta dos licitantes convocados para apresentação de propostas, após a fase de envio de lances.
- 4.11. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo ou o seu percentual de desconto máximo quando do cadastramento da proposta e obedecerá às seguintes regras:
- 4.11.1. a aplicação do intervalo mínimo de diferença de valores ou de percentuais entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
- 4.11.2. os lances serão de envio automático pelo sistema, respeitado o valor final mínimo, caso estabelecido, e o intervalo de que trata o subitem acima.
- 4.12. O valor final mínimo ou o percentual de desconto final máximo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:
- 4.12.1. valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço; e
- 4.12.2. percentual de desconto inferior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por maior desconto.
- 4.13. O valor final mínimo ou o percentual de desconto final máximo parametrizado na forma do item 4.11 possuirá caráter sigiloso para os demais fornecedores e para o órgão ou entidade promotora da licitação, podendo ser disponibilizado estrita e permanentemente aos órgãos de controle externo e interno.
- 4.14. 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.
- 4.15. O licitante deverá comunicar imediatamente ao provedor do sistema qualquer acontecimento que possa comprometer o sigilo ou a segurança, para imediato bloqueio de acesso.

5. DO PREENCHIMENTO DA PROPOSTA

- 5.1. O licitante deverá enviar sua proposta mediante o preenchimento, no sistema eletrônico, dos seguintes campos:

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

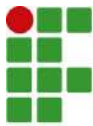
- 5.1.1. *valor unitário do item;*
- 5.1.2. *Marca;*
- 5.1.3. *Fabricante;*
- 5.2. Todas as especificações do objeto contidas na proposta vinculam o licitante.
 - 5.2.1. O licitante NÃO poderá oferecer proposta em quantitativo inferior ao máximo previsto para contratação.
- 5.3. Nos valores propostos estarão inclusos todos os custos operacionais, encargos previdenciários, trabalhistas, tributários, comerciais e quaisquer outros que incidam direta ou indiretamente na execução do objeto.
- 5.4. 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.
- 5.5. Se o regime tributário da empresa implicar o recolhimento de tributos em percentuais variáveis, a cotação adequada será a que corresponde à média dos efetivos recolhimentos da empresa nos últimos doze meses.
- 5.6. Independentemente do percentual de tributo inserido na planilha, no pagamento serão retidos na fonte os percentuais estabelecidos na legislação vigente.
- 5.7. Na presente licitação, a Microempresa e a Empresa de Pequeno Porte poderão se beneficiar do regime de tributação pelo Simples Nacional.
- 5.8. 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.
- 5.9. O prazo de validade da proposta não será inferior a **60 (sessenta)** dias, a contar da data de sua apresentação.
- 5.10. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;
 - 5.10.1. Caso o critério de julgamento seja o de maior desconto, o preço já decorrente da aplicação do desconto ofertado deverá respeitar os preços máximos previstos no item 4.9.
- 5.11. O descumprimento das regras supramencionadas pela Administração por parte dos contratados pode ensejar a responsabilização pelo Tribunal de Contas da União 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.

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

- 6.1. 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.
- 6.2. Os licitantes poderão retirar ou substituir a proposta ou os documentos de habilitação, quando for o caso, anteriormente inseridos no sistema, até a abertura da sessão pública.
- 6.3. O sistema disponibilizará campo próprio para troca de mensagens entre o Pregoeiro e os licitantes.
- 6.4. 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.
- 6.5. O lance deverá ser ofertado pelo valor unitário do item.
- 6.6. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.
- 6.7. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.
- 6.8. 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 0,1% (um décimo por cento).
- 6.9. O licitante poderá, uma única vez, excluir seu último lance ofertado, no intervalo de quinze segundos após o registro no sistema, na hipótese de lance inconsistente ou inexequível.
- 6.10. O procedimento seguirá de acordo com o modo de disputa adotado.
- 6.11. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto”, os licitantes apresentarão lances públicos e sucessivos, com prorrogações.
 - 6.11.1. 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.
 - 6.11.2. 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.
 - 6.11.3. 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.
 - 6.11.4. 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.
 - 6.11.5.** Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 6.12. Caso seja adotado para o envio de lances no pregão eletrônico o modo de disputa “aberto e fechado”, os licitantes apresentarão lances públicos e sucessivos, com lance final e fechado.
- 6.12.1. A etapa de lances da sessão pública terá duração inicial de quinze minutos. Após esse prazo, o sistema encaminhará aviso de fechamento iminente dos lances, após o que transcorrerá o período de até dez minutos, aleatoriamente determinado, findo o qual será automaticamente encerrada a recepção de lances.
- 6.12.2. Encerrado o prazo previsto no subitem anterior, o sistema abrirá oportunidade para que o autor da oferta de valor mais baixo e os das ofertas com preços até 10% (dez por cento) superiores àquela possam ofertar um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
- 6.12.3. No procedimento de que trata o subitem supra, o licitante poderá optar por manter o seu último lance da etapa aberta, ou por ofertar melhor lance.
- 6.12.4. Não havendo pelo menos três ofertas nas condições definidas neste item, poderão os autores dos melhores lances subsequentes, na ordem de classificação, até o máximo de três, oferecer um lance final e fechado em até cinco minutos, o qual será sigiloso até o encerramento deste prazo.
- 6.12.5. Após o término dos prazos estabelecidos nos itens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 6.13. Após o término dos prazos estabelecidos nos subitens anteriores, o sistema ordenará e divulgará os lances segundo a ordem crescente de valores.
- 6.14. Não serão aceitos dois ou mais lances de mesmo valor, prevalecendo aquele que for recebido e registrado em primeiro lugar.
- 6.15. Durante o transcurso da sessão pública, os licitantes serão informados, em tempo real, do valor do menor lance registrado, vedada a identificação do licitante.
- 6.16. 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.
- 6.17. 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.
- 6.18. Caso o licitante não apresente lances, concorrerá com o valor de sua proposta.
- 6.19. Em relação a itens não exclusivos para participação de microempresas e empresas de pequeno porte, uma vez encerrada a etapa de lances, será efetivada a verificação automática, junto à Receita Federal, do porte da entidade empresarial. O sistema identificará em coluna própria as microempresas e empresas de pequeno porte participantes, procedendo à comparação com os valores da primeira colocada, se esta for empresa de maior porte, assim como das demais classificadas, para o fim de aplicar-se o disposto nos [arts. 44 e 45 da Lei Complementar nº 123, de 2006](#), regulamentada pelo [Decreto nº 8.538, de 2015](#).



EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 6.19.1. Nessas condições, as propostas de microempresas e empresas de pequeno porte que se encontrarem na faixa de até 5% (cinco por cento) acima da melhor proposta ou melhor lance serão consideradas empatadas com a primeira colocada.
- 6.19.2. A melhor classificada nos termos do subitem anterior terá o direito de encaminhar uma última oferta para desempate, obrigatoriamente em valor inferior ao da primeira colocada, no prazo de 5 (cinco) minutos controlados pelo sistema, contados após a comunicação automática para tanto.
- 6.19.3. Caso a microempresa ou a empresa de pequeno porte melhor classificada desista ou não se manifeste no prazo estabelecido, serão convocadas as demais licitantes microempresa e empresa de pequeno porte que se encontrem naquele intervalo de 5% (cinco por cento), na ordem de classificação, para o exercício do mesmo direito, no prazo estabelecido no subitem anterior.
- 6.19.4. No caso de equivalência dos valores apresentados pelas microempresas e empresas de pequeno porte que se encontrem nos intervalos estabelecidos nos subitens anteriores, será realizado sorteio entre elas para que se identifique aquela que primeiro poderá apresentar melhor oferta.
- 6.20. Será assegurado o direito de preferência previsto no artigo 3º da Lei nº 8.248, de 1991, conforme procedimento estabelecido nos artigos 5º e 8º do Decreto nº 7.174, de 2010, nos seguintes termos:
- 6.20.1. Após a aplicação das regras de preferência para microempresas e empresas de pequeno porte, caberá a aplicação das regras de preferência, sucessivamente, para:
- 6.20.1.1. bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;
- 6.20.1.2. bens e serviços com tecnologia desenvolvida no País; e
- 6.20.1.3. bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal, nos termos do art. 5º e 8º do Decreto 7.174, de 2010 e art. 3º da Lei nº 8.248, de 1991.
- 6.20.2. Os licitantes classificados que estejam enquadrados no item 6.21.1.1, na ordem de classificação, serão convocados para que possam oferecer nova proposta ou novo lance para igualar ou superar a melhor proposta válida, caso em que será declarado vencedor do certame.
- 6.20.3. Caso a preferência não seja exercida na forma do item 6.21.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.21.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 6.21.1.3 caso esse direito não seja exercido.
- 6.20.4.** As licitantes qualificadas como microempresas ou empresas de pequeno porte que fizerem jus ao direito de preferência previsto no Decreto nº 7.174, de 2010, terão prioridade no exercício desse benefício em relação às médias e às grandes empresas na mesma situação.
- 6.21. Só poderá haver empate entre propostas iguais (não seguidas de lances), ou entre lances finais da fase fechada do modo de disputa aberto e fechado.



EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 6.21.1. Havendo eventual empate entre propostas ou lances, o critério de desempate será aquele previsto no [art. 60 da Lei nº 14.133, de 2021](#), nesta ordem:
- 6.21.1.1. disputa final, hipótese em que os licitantes empatados poderão apresentar nova proposta em ato contínuo à classificação;
 - 6.21.1.2. 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;
 - 6.21.1.3. desenvolvimento pelo licitante de ações de equidade entre homens e mulheres no ambiente de trabalho, conforme regulamento;
 - 6.21.1.4. desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.
- 6.21.2. Persistindo o empate, será assegurada preferência, sucessivamente, aos bens e serviços produzidos ou prestados por:
- 6.21.2.1. 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;
 - 6.21.2.2. empresas brasileiras;
 - 6.21.2.3. empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;
 - 6.21.2.4. empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).
- 6.22. 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 poderá negociar condições mais vantajosas, após definido o resultado do julgamento.
- 6.22.1. Não será admitida a previsão de preços diferentes em razão de local de entrega ou de acondicionamento, tamanho de lote ou qualquer outro motivo.
 - 6.22.2. 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.
 - 6.22.3. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.
 - 6.22.4. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.
 - 6.22.5. O pregoeiro 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,

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.22.6. É facultado ao pregoeiro prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

6.23. Após a negociação do preço, o Pregoeiro iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, 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:

7.1.1. SICAF;

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

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

7.2. 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 nº 8.429, de 1992](#).

7.3. Caso conste na Consulta de Situação do licitante a existência de Ocorrências Impeditivas Indiretas, o Pregoeiro diligenciará para verificar se houve fraude por parte das empresas apontadas no Relatório de Ocorrências Impeditivas Indiretas. ([IN nº 3/2018, art. 29, caput](#))

7.3.1. A tentativa de burla será verificada por meio dos vínculos societários, linhas de fornecimento similares, dentre outros. ([IN nº 3/2018, art. 29, §1º](#)).

7.3.2. O licitante será convocado para manifestação previamente a uma eventual desclassificação. ([IN nº 3/2018, art. 29, §2º](#)).

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

7.4. Caso atendidas as condições de participação, será iniciado o procedimento de habilitação.

7.5. Caso o licitante provisoriamente classificado em primeiro lugar tenha se utilizado de algum tratamento favorecido às ME/EPPs, o pregoeiro verificará se faz jus ao benefício, em conformidade com os itens 3.5.1 e 4.6 deste edital.

7.6. Para os itens enquadrados no Anexo I da Instrução Normativa IBAMA nº 06, de 15/03/2013, o Pregoeiro solicitará ao licitante provisoriamente classificado em primeiro lugar que apresente ou envie juntamente com a proposta, sob pena de não-aceitação, o Comprovante de Registro do fabricante do produto no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, acompanhado do respectivo Certificado de Regularidade válido, nos termos do

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

artigo 17, inciso II, da Lei nº 6.938, de 1981, e da Instrução Normativa IBAMA nº 06, de 15/03/2013, e legislação correlata.

7.6.1. A apresentação do Certificado de Regularidade será dispensada, caso o Pregoeiro logre êxito em obtê-lo mediante consulta on line ao sítio oficial do IBAMA, anexando-o ao processo;"

7.7. 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, observado o disposto no [artigo 29 a 35 da IN SEGES nº 73, de 30 de setembro de 2022](#).

7.8. Será desclassificada a proposta vencedora que:

7.8.1. conter vícios insanáveis;

7.8.2. não obedecer às especificações técnicas contidas no Termo de Referência;

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

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

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

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

7.9.1. A inexecuibilidade, na hipótese de que trata o **caput**, só será considerada após diligência do pregoeiro, que comprove:

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

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

7.10. Se houver indícios de inexecuibilidade 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.

7.11. Para fins de análise da proposta quanto ao cumprimento das especificações do objeto, poderá ser colhida a manifestação escrita do setor requisitante do serviço ou da área especializada no objeto.

8. DA FASE DE HABILITAÇÃO

8.1. Os documentos previstos no Termo de Referência, necessários e suficientes para demonstrar a capacidade do licitante de realizar o objeto da licitação, serão exigidos para fins de habilitação, nos termos dos [arts. 62 a 70 da Lei nº 14.133, de 2021](#).

8.1.1. A documentação exigida para fins de habilitação jurídica, fiscal, social e trabalhista e econômico-financeira, poderá ser substituída pelo registro cadastral no SICAF.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 8.2. 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.
- 8.3. 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.
- 8.4. Quando permitida a participação de consórcio de empresas, a habilitação técnica, quando exigida, será feita por meio do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, quando exigida, será observado o somatório dos valores de cada consorciado.
- 8.4.1. Se o consórcio não for formado integralmente por microempresas ou empresas de pequeno porte e o termo de referência exigir requisitos de habilitação econômico-financeira, haverá um acréscimo de 10% para o consórcio em relação ao valor exigido para os licitantes individuais.
- 8.5. Os documentos exigidos para fins de habilitação poderão ser apresentados em original, por cópia, inclusive autenticada ou assinada digitalmente, desde que seja possível o rastreamento da origem.
- 8.6. Os documentos exigidos para fins de habilitação poderão ser substituídos por registro cadastral emitido por órgão ou entidade pública, desde que o registro tenha sido feito em obediência ao disposto na Lei nº 14.133/2021.
- 8.7. Será verificado se o licitante apresentou declaração de que atende aos requisitos de habilitação, e o declarante responderá pela veracidade das informações prestadas, na forma da lei ([art. 63, I, da Lei nº 14.133/2021](#)).
- 8.8. Será verificado se o licitante apresentou no sistema, sob pena de inabilitação, a declaração de que 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.
- 8.9. O licitante deverá apresentar, sob pena de desclassificação, 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.
- 8.10. A habilitação será verificada por meio do Sicaf, nos documentos por ele abrangidos.
- 8.10.1. 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](#)).
- 8.11. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicaf 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. ([IN nº 3/2018, art. 7º, caput](#)).

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 8.11.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. ([IN nº 3/2018, art. 7º, parágrafo único](#)).
- 8.12. A verificação pelo pregoeiro, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.
- 8.12.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicaf serão enviados por meio do sistema, em formato digital, no prazo de, NO MÍNIMO, DUAS HORAS, prorrogável por igual período, contado da solicitação do pregoeiro.
- 8.12.2. Na hipótese de a fase de habilitação anteceder a fase de apresentação de propostas e lances, os licitantes encaminharão, por meio do sistema, simultaneamente os documentos de habilitação e a proposta com o preço ou o percentual de desconto, observado o disposto no [§ 1º do art. 36 e no § 1º do art. 39 da Instrução Normativa SEGES nº 73, de 30 de setembro de 2022](#).
- 8.13. A verificação no Sicaf ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.
- 8.13.1. Os documentos relativos à regularidade fiscal que constem do Termo de Referência somente serão exigidos, em qualquer caso, em momento posterior ao julgamento das propostas, e apenas do licitante mais bem classificado.
- 8.13.2. Respeitada a exceção do subitem anterior, relativa à regularidade fiscal, quando a fase de habilitação anteceder as fases de apresentação de propostas e lances e de julgamento, a verificação ou exigência do presente subitem ocorrerá em relação a todos os licitantes.
- 8.14. Após a entrega dos documentos para 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](#)):
- 8.14.1. complementação de informações acerca dos documentos já apresentados pelos licitantes e desde que necessária para apurar fatos existentes à época da abertura do certame; e
- 8.14.2. atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;
- 8.15. Na análise dos documentos de habilitação, a comissão de contratação 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.
- 8.16. 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 8.13.1.
- 8.17. 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.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 8.18. A comprovação de regularidade fiscal e trabalhista das microempresas e das empresas de pequeno porte somente será exigida para efeito de contratação, e não como condição para participação na licitação ([art. 4º do Decreto nº 8.538/2015](#)).
- 8.19. Quando a fase de habilitação anteceder a de julgamento e já tiver sido encerrada, não caberá exclusão de licitante por motivo relacionado à habilitação, salvo em razão de fatos supervenientes ou só conhecidos após o julgamento.

9. DA ATA DE REGISTRO DE PREÇOS

- 9.1. Homologado o resultado da licitação, o licitante mais bem classificado terá o prazo de 05 (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.
- 9.1.1. Alternativamente à convocação para comparecer perante o órgão ou entidade para a assinatura da Ata de Registro de Preços, a Administração poderá encaminhá-la para assinatura, mediante correspondência postal com aviso de recebimento (AR) ou meio eletrônico, para que seja assinada e devolvida no prazo de 05 (cinco) dias, a contar da data de seu recebimento.
- 9.2. 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:
- 9.2.1. a solicitação seja devidamente justificada e apresentada dentro do prazo; e
- 9.2.2. a justificativa apresentada seja aceita pela Administração.
- 9.3. A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no sistema de registro de preços.
- 9.4. 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.
- 9.5. O preço registrado, com a indicação dos fornecedores, será divulgado no PNCP e disponibilizado durante a vigência da ata de registro de preços.
- 9.6. 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 aquisição pretendida, desde que devidamente justificada.
- 9.7. 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.

10. DA FORMAÇÃO DO CADASTRO DE RESERVA

- 10.1. Após a homologação da licitação, será incluído na ata, na forma de anexo, o registro:
- 10.1.1. dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e
 - 10.1.2. dos licitantes que mantiverem sua proposta original.
- 10.2. Será respeitada, nas contratações, a ordem de classificação dos licitantes ou fornecedores registrados na ata.
- 10.2.1. A apresentação de novas propostas na forma deste item não prejudicará o resultado do certame em relação ao licitante mais bem classificado.
 - 10.2.2. 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.
- 10.3. A habilitação dos licitantes que comporão o cadastro de reserva será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:
- 10.3.1. quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou
 - 10.3.2. 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.
- 10.4. 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:
- 10.4.1. 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
 - 10.4.2. adjudicar e firmar o contrato nas condições ofertadas pelos licitantes remanescentes, observada a ordem de classificação, quando frustrada a negociação de melhor condição.

11. DOS RECURSOS

- 11.1.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](#).
- 11.2.O prazo recursal é de 3 (três) dias úteis, contados da data de intimação ou de lavratura da ata.
- 11.3.Quando o recurso apresentado impugnar o julgamento das propostas ou o ato de habilitação ou inabilitação do licitante:

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 11.3.1. a intenção de recorrer deverá ser manifestada imediatamente, sob pena de preclusão;
- 11.3.1.1. o prazo para a manifestação da intenção de recorrer não será inferior a 10 (dez) minutos.
- 11.3.2. o prazo para apresentação das razões recursais será iniciado na data de intimação ou de lavratura da ata de habilitação ou inabilitação;
- 11.3.3. na hipótese de adoção da inversão de fases prevista no [§ 1º do art. 17 da Lei nº 14.133, de 2021](#), o prazo para apresentação das razões recursais será iniciado na data de intimação da ata de julgamento.
- 11.4. Os recursos deverão ser encaminhados em campo próprio do sistema.
- 11.5. 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.
- 11.6. Os recursos interpostos fora do prazo não serão conhecidos.
- 11.7. 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.
- 11.8. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.
- 11.9. O acolhimento do recurso invalida tão somente os atos insuscetíveis de aproveitamento.
- 11.10. Os autos do processo permanecerão com vista franqueada aos interessados, no endereço constante neste Edital.

12. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES

- 12.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:
- 12.1.1. 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;
- 12.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não manter a proposta em especial quando:
- 12.1.2.1. não enviar a proposta adequada ao último lance ofertado ou após a negociação;
- 12.1.2.2. recusar-se a enviar o detalhamento da proposta quando exigível;
- 12.1.2.3. pedir para ser desclassificado quando encerrada a etapa competitiva; ou
- 12.1.2.4. deixar de apresentar amostra;
- 12.1.2.5. apresentar proposta ou amostra em desacordo com as especificações do edital;

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 12.1.3. não celebrar o contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;
 - 12.1.3.1. 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;
- 12.1.4. apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação;
- 12.1.5. fraudar a licitação;
- 12.1.6. comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:
 - 12.1.6.1. agir em conluio ou em desconformidade com a lei;
 - 12.1.6.2. induzir deliberadamente a erro no julgamento;
 - 12.1.6.3. apresentar amostra falsificada ou deteriorada;
- 12.1.7. praticar atos ilícitos com vistas a frustrar os objetivos da licitação
- 12.1.8. praticar ato lesivo previsto no [art. 5º da Lei n.º 12.846, de 2013](#).
- 12.2. Com fulcro na [Lei nº 14.133, de 2021](#), a Administração poderá, garantida a prévia defesa, aplicar aos licitantes e/ou adjudicatários as seguintes sanções, sem prejuízo das responsabilidades civil e criminal:
 - 12.2.1. advertência;
 - 12.2.2. multa;
 - 12.2.3. impedimento de licitar e contratar e
 - 12.2.4. 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.
- 12.3. Na aplicação das sanções serão considerados:
 - 12.3.1. a natureza e a gravidade da infração cometida.
 - 12.3.2. as peculiaridades do caso concreto
 - 12.3.3. as circunstâncias agravantes ou atenuantes
 - 12.3.4. os danos que dela provierem para a Administração Pública
 - 12.3.5. a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.
- 12.4. A multa será recolhida em percentual de 0,5% a 30% incidente sobre o valor do contrato licitado, recolhida no prazo máximo de **30 (trinta) dias** úteis, a contar da comunicação oficial.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 12.4.1. Para as infrações previstas nos itens 12.1.1, 12.1.2 e 12.1.3, a multa será de **10%** do valor do contrato licitado.
- 12.4.2. Para as infrações previstas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, a multa será de 20% do valor do contrato licitado.
- 12.5. 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.
- 12.6. 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.
- 12.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 12.1.1, 12.1.2 e 12.1.3, 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.
- 12.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar, em decorrência da prática das infrações dispostas nos itens 12.1.4, 12.1.5, 12.1.6, 12.1.7 e 12.1.8, bem como pelas infrações administrativas previstas nos itens 12.1.1, 12.1.2 e 12.1.3 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](#).
- 12.9. 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 12.1.3, 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](#).
- 12.10. 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.
- 12.11. 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.
- 12.12. 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.
- 12.13. O recurso e o pedido de reconsideração terão efeito suspensivo do ato ou da decisão recorrida até que sobrevenha decisão final da autoridade competente.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

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

13. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

- 13.1. 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.
- 13.2. A resposta à impugnação ou ao pedido de esclarecimento será divulgada em sítio eletrônico oficial no prazo de até 3 (três) dias úteis, limitado ao último dia útil anterior à data da abertura do certame.
- 13.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica para o e-mail licitacoes@ifsc.edu.br.
- 13.4. As impugnações e pedidos de esclarecimentos não suspendem os prazos previstos no certame.
- 13.4.1. A concessão de efeito suspensivo à impugnação é medida excepcional e deverá ser motivada pelo agente de contratação, nos autos do processo de licitação.
- 13.5. Acolhida a impugnação, será definida e publicada nova data para a realização do certame.

14. DAS DISPOSIÇÕES GERAIS

- 14.1. Será divulgada ata da sessão pública no sistema eletrônico.
- 14.2. 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.
- 14.3. Todas as referências de tempo no Edital, no aviso e durante a sessão pública observarão o horário de Brasília - DF.
- 14.4. A homologação do resultado desta licitação não implicará direito à contratação.
- 14.5. 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.
- 14.6. 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.
- 14.7. 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.

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

- 14.8. 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.
- 14.9. Em caso de divergência entre disposições deste Edital e de seus anexos ou demais peças que compõem o processo, prevalecerá as deste Edital.
- 14.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico <https://www.gov.br/compras/pt-br/>, <https://sig.ifsc.edu.br/public/listaEditais.do?tipo=1&aba=p-comunicados> e também poderá ser lido e/ou obtido no endereço Rua 14 de Julho, 150, Coqueiros, Fpolis/SC 88075-010 (Departamento de Compras do IFSC), mediante prévio agendamento por e-mail, nos dias úteis, no horário das 08 horas às 17 horas, mesmo endereço e período no qual os autos do processo administrativo permanecerão com vista franqueada aos interessados mediante prévio agendamento pelo e-mail licitacoes@ifsc.edu.br.
- 14.11. Integram este Edital, para todos os fins e efeitos, os seguintes anexos:
- 14.11.1. ANEXO I - Termo de Referência
 - 14.11.1.1. Apêndice do Anexo I – Termo de Referência
 - 14.11.1.2. Apêndice do Anexo I – Estudo Técnico Preliminar
 - 14.11.1.3. Apêndice do Anexo I – Quadro de Especificações Mínimas
 - 14.11.1.4. Apêndice do Anexo I – Relatório de Requisições
 - 14.11.1.5. Apêndice do Anexo I – Pesquisa de Preço
 - 14.11.2. ANEXO II – Minuta de Termo de Contrato
 - 14.11.3. ANEXO III – Ordem de Serviço ou de Fornecimento de Bens
 - 14.11.4. ANEXO IV – Termo de Recebimento Provisório – Serviços de Tic
 - 14.11.5. ANEXO V – Termo de Recebimento Definitivo
 - 14.11.6. ANEXO VI – Minuta da Ata de Registro de Preços

Florianópolis, 21 de dezembro de 2023

ALOISIO SILVA JUNIOR

EDITAL - PREGÃO ELETRÔNICO Nº 31009/2023

Pró-Reitor de Administração

TERMO DE REFERÊNCIA COMPRAS DE TIC – LEI 14.133/2021

(Processo Administrativo nº 23292.034402/2023-70)

Referência: Arts. 12 a 24 da Instrução Normativa SGD/ME nº 94, de 2022

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Aquisição de AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TI, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

ITEM	ESPECIFICAÇÃO	CATMAT	UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
NÃO ASSOCIADO(S) A LOTE/GRUPO						
01	ADAPTADOR DE TELEFONIA ANALÓGICA COM PORTAS FXS/FXO	348831	UNIDADE	50	928,00	46.400,00
26	SERVIDOR EM LÂMINA	452929	UNIDADE	7	247.316,67	1.731.216,69
38	USER MEDIA GATEWAY - VOIP	348826	UNIDADE	2	3.907,13	7.814,26
LOTE/GRUPO 1: REDE SEM FIO						
05	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA	605537	UNIDADE	50	1.510,75	75.537,50
09	PONTO DE ACESSO INDOOR - TIPO I - SOLUÇÃO DE SEGURANÇA DE DADOS	484745	UNIDADE	100	6.095,48	609.548,00
10	PONTO DE ACESSO INDOOR - TIPO II - SOLUÇÃO DE SEGURANÇA DE DADOS	484745	UNIDADE	40	10.293,39	411.735,60
11	PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE SEGURANÇA DE DADOS	484745	UNIDADE	10	11.072,04	110.720,40
20	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO I	27260	UNIDADE	100	1.300,11	130.011,00
21	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO II	27260	UNIDADE	40	2.195,43	87.817,20
22	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT OUTDOOR	27260	UNIDADE	10	2.361,56	23.615,60
25	SERVIÇO TÉCNICO PARA SITE SURVEY - SOLUÇÃO DE SEGURANÇA DE DADOS	27260	UNIDADE	12	9.674,02	116.088,24
ITEM	ESPECIFICAÇÃO		UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

LOTE/GRUPO 2: CONEXÃO DE REDE						
23	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 1	27260	UNIDADE	4	6.139,86	24.559,44
24	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 2	27260	UNIDADE	4	8.863,76	35.455,04
31	SWITCH CORE - TIPO 1 – SOLUÇÃO DE SEGURANÇA DADOS	609334	UNIDADE	4	28.677,61	114.710,44
32	SWITCH CORE - TIPO 2 – SOLUÇÃO DE SEGURANÇA DE DADOS	604753	UNIDADE	4	41.400,18	165.600,72
33	SWITCH CORE TIPO 3 – SOLUÇÃO DE SEGURANÇA DE DADOS	609334	UNIDADE	2	164.139,38	328.278,76
34	TRANSCEIVER 10GBASE-LR - SOLUÇÃO DE SEGURANÇA DE DADOS	609338	UNIDADE	20	3.377,76	67.555,20
35	TRANSCEIVER 10GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS	462427	UNIDADE	20	1.196,15	23.923,00
36	TRANSCEIVER 40GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS	462427	UNIDADE	10	30.930,54	309.305,40
LOTE/GRUPO 3: SEGURANÇA DE REDE						
04	FONTE HOT SWAPPABLE - FORTIGATE 600E	603556	UNIDADE	4	8.773,50	35.094,00
06	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE 60F	27499	UNIDADE	6	12.505,08	75.030,48
07	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-100F	27499	UNIDADE	1	42.246,77	42.246,77
08	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-80F	27499	UNIDADE	5	21.545,87	107.729,35
12	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3	27260	UNIDADE	16	10.084,63	161.354,08
13	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4	27260	UNIDADE	5	11.148,61	55.743,05
14	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5	27260	UNIDADE	4	11.762,52	47.050,08
15	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6	27260	UNIDADE	2	13.716,78	27.433,56

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

ITEM	ESPECIFICAÇÃO		UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
16	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3	27260	UNIDADE	16	20.446,53	327.144,48
17	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4	27260	UNIDADE	5	40.091,21	200.456,05
18	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5	27260	UNIDADE	4	74.088,60	296.354,40
19	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6	27260	UNIDADE	2	202.947,00	405.894,00
27	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 3	481646	UNIDADE	16	14.395,43	230.326,88
28	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 4	481646	UNIDADE	05	28.226,36	141.131,80
29	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 5	481646	UNIDADE	4	52.162,32	208.649,28
30	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 6	481646	UNIDADE	2	180.481,52	360.963,04
37	TREINAMENTO – SOLUÇÃO DE SEGURANÇA DE DADOS	21172	SERVIÇO	1	7.278,28	7.278,28
LOTE/GRUPO 4: BACKUP DE DADOS - COM PARTICIPANTE EXTERNO NO ITEM 03						
2	APPLIANCE DE BACKUP - TIPO 1	479950	UNIDADE	2	630.484,09	1.260.968,18
3	APPLIANCE DE BACKUP - TIPO 2	479950	UNIDADE	3	745.295,29	2.235.885,87
VALOR TOTAL				R\$ 10.646.626,12		

- 1.2. O objeto desta contratação não se enquadra como sendo de bem de luxo, conforme [Decreto nº 10.818, de 27 de setembro de 2021](#).
- 1.3. Os bens objetos desta contratação são caracterizados como comuns, dada a existência de padrões de mercado que permitem a fixação de critérios de qualidade e de desempenho.
- 1.4. O objeto da contratação não incide nas hipóteses vedadas pelos artigos 3º e 4º da IN SGD nº 94/2022.
- 1.5. O objeto da contratação incide nas hipóteses vedadas pelo ANEXO I - CONTRATAÇÃO DE INFRAESTRUTURA DE CENTRO DE DADOS, SERVIÇOS EM NUVEM, SALA-COFRE E SALA SEGURA - da IN SGD nº 94/2022.
- Entretanto, o ETP indica a viabilidade da contratação on-premise em função de que o equipamento atual ainda está com suporte ativo e os servidores (item 25) são componentes da solução e não a

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

solução como um todo. Além disso, é demonstrada a vantagem financeira em relação à contratação em nuvem.

- 1.6. O objeto da contratação atende ao ANEXO I - AQUISIÇÕES DE ATIVOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO - da IN SGD nº 94/2022.
- 1.7. A administração observou os guias, manuais e modelos publicados pelo Órgão Central do SISP.
- 1.8. Para este processo considera-se a necessidade de indicação de fabricantes, em atendimento ao art. 41, inciso I, alíneas a, b e d:
 - 1.8.1. Grupos 1,2 e 3 - FABRICANTE: FORTINET - MOTIVO: art. 41, inciso I, alíneas “a” e “b”.
 - 1.8.2. Grupo 4 - FABRICANTE: EXAGRID - MOTIVO: art. 41, inciso I, alíneas “a” e “d”.
 - 1.8.3. Item 26 - FABRICANTE: HPE - MOTIVO: art. 41, inciso I, alíneas “a” e “b”.

2. DESCRIÇÃO DA SOLUÇÃO COMO UM TODO CONSIDERADO O CICLO DE VIDA DO OBJETO E ESPECIFICAÇÃO DO PRODUTO

- 2.1. Os equipamentos devem atender os critérios na Portaria nº 170, de 10 de abril de 2012, do Inmetro (<http://www.inmetro.gov.br/legislacao/rtac/pdf/rtac001808.pdf>), conforme a seguir:
 - 2.1.1. Servidores (*blades, appliance de backup*): comprovar que atendem os requisitos de segurança e compatibilidade eletromagnética.
- 2.2. A descrição da solução como um todo encontra-se pormenorizada em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.
- 2.3. A descrição de cada equipamento encontra-se no Quadro de Especificações Mínimas, apêndice deste Termo de Referência.
- 2.4. Os itens deste projeto não fazem parte do escopo da PORTARIA SGD/MGI Nº 2.715, DE 21 DE JUNHO DE 2023;
- 2.5. Os itens deste projeto não fazem parte do escopo da PORTARIA SGD/MGI Nº 5.950, DE 26 DE OUTUBRO DE 2023;
- 2.6. A solução de TIC consiste na AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TI.
- 2.7. Justificativa:
 - 2.7.1. O Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina (IFSC) é uma das instituições que compõem a Rede Federal de Educação Profissional, Científica e Tecnológica (RFEPT) com a finalidade de ofertar formação e qualificação em diversas áreas, nos vários níveis e modalidades de ensino, bem como realizar pesquisa e extensão. Atualmente o IFSC é composto por vinte e um câmpus (Araranguá, Caçador, Canoinhas, Chapecó, Criciúma, Florianópolis, Florianópolis-Continente, Garopaba, Gaspar, Jaraguá do Sul-Centro, Jaraguá do Sul-Rau, Itajaí, Joinville, Lages, São José, Palhoça Bilingue, São Carlos, São Miguel do Oeste, Tubarão, Urupema e Xanxerê, além do Câmpus Avançado São Lourenço do Oeste) um polo de inovação, além da reitoria, localizada em Florianópolis.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

A aquisição dos equipamentos, objetos deste termo, servirá para ampliar o parque tecnológico da instituição com foco na segurança da informação (*firewall*, *appliance* para backup seguro, rede sem fio e *switches core*).

2.7.2. Quantitativo: Estimativa realizada pela Diretoria de TIC com base nas suas necessidades e na conclusão do projeto Conecta IFSC. As requisições foram cadastradas no sistema SIG/SIPAC, disponível no item 1.1 e na documentação que compõe este processo. O quantitativo está detalhado em tópico específico dos Estudos Técnicos Preliminares, apêndice deste Termo de Referência.

2.8. Características gerais da solução:

2.8.1. Quando não especificadas exceções, não serão admitidos equipamentos modificados através de adaptadores, fresagens, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou qualquer outro procedimento ou emprego de materiais inadequados que adaptem forçadamente o equipamento ou suas partes que sejam fisicamente ou logicamente incompatíveis;

2.8.2. Todos os equipamentos a serem entregues deverão ser idênticos, ou seja, todos os componentes externos e internos devem ser dos mesmos modelos e marcas constantes na proposta comercial. Caso o componente não mais se encontre disponível no mercado, admite-se substituições por componente com qualidade e características idênticas ou superiores, desde que aceito pelo CONTRATANTE, mediante nova homologação;

2.8.3. Deverão ser entregues todos os cabos, drivers e manuais necessários à sua instalação bem como a de seus componentes. Todos os cabos necessários ao funcionamento dos equipamentos deverão ser fornecidos.

2.8.4. Todos os equipamentos deverão ser entregues devidamente acondicionadas em embalagens individuais adequadas, de forma a garantir a máxima proteção durante o transporte e a armazenagem;

2.8.5. O item 25 inclui na proposta de preços a instalação e configuração do servidor na infraestrutura do IFSC.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. O quantitativo de cada item da solução está descrito no Estudo Técnico Preliminar, apêndice deste termo de referência.

3.2. Este processo de contratação resultará na formação de Ata de Registro de Preços (ARP), prevendo-se a renovação da ARP e considerando-se a utilização de orçamentos de 2024 - 2025 (primeiro ano da ARP) e 2025 - 2026 (segundo ano da ARP).

3.3. A adesão a ARP por outros órgãos justifica-se pela possível economicidade que trará ao IFSC visto que o volume maior de possíveis aquisições tenderá a baixar o valor das propostas apresentadas.

3.3.1. Poderão aderir a Ata de Registro de Preços os órgãos não participantes, observados os seguintes requisitos:

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 3.3.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
- 3.3.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei 14.133;
- 3.3.1.3. prévias consulta e aceitação do órgão ou entidade gerenciadora e do fornecedor.
- 3.3.1.4. O órgão ou entidade interessada em aderir à Ata de Registro de Preços deverá registrar no Estudo Técnico Preliminar o ganho de eficiência, a viabilidade e a economicidade para a administração pública federal da utilização da ata de registro de preços, conforme o disposto no § 2º do art. 86 da Lei nº 14.133, de 2021.
- 3.3.2. O órgão ou entidade interessada em participar de uma contratação conjunta no Sistema de Registro de Preços deverá fundamentar a compatibilidade do seu Estudo Técnico Preliminar e demais documentos de planejamento da contratação com o Termo de Referência do órgão gerenciador.
- 3.4. O objeto da contratação está previsto no Plano de Contratações Anual (PCA) 2023, conforme consta das informações básicas deste termo de referência e possui DFD cadastrada para o PCA 2024.

Documento de Formalização de Demanda	Unidade (Uorg)	Investimento Previsto
13/2022	Diretoria de Tecnologia da Informação e Comunicação	R\$ 399.675,00
27/2023	Diretoria de Tecnologia da Informação e Comunicação	R\$ 393.419,16

O objeto da contratação está previsto no Plano de Contratações Anual 2023, conforme detalhamento a seguir:

- I) ID PCA no PNCP: 11402887000160-0-000001/2023.
- II) Data de publicação no PNCP: 04/07/2023.
- III) Id do item no PCA: 2752/2022.
- IV) Classe/Grupo: 750.
- V) Identificador da Futura Contratação: 90158/2022.
- 3.5. Justificativa da diferença de valor atribuído no PCA e do valor total do processo.
- A diferença de valor se dá com base no orçamento anual definido para aquisições de TIC para a Diretoria de Tecnologia da Comunicação e Informação (DTIC), sem considerar recursos dos câmpus e extra orçamentários como o Termo de Execução Descentralizada (TED).

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Em 2022 o investimento direto da DTIC foi de R\$ 316.858,43. Entretanto, foi investido R\$ 2.298.802,00 com recurso de TED e R\$ 3.465.237,89 com recursos dos câmpus. Os apontamentos aqui apresentados referem-se apenas a investimento (aquisições de bens).

No total, em 2022, foram investidos em TIC (aquisição de bens): **R\$ 6.080.898,32**. Se for considerado investimento e custeio, o valor total investido foi de **R\$ 6.880.943,93**

Em 2023 foram recebidos valores de TED na ordem de R\$ 3.405.890,67, além do orçamento próprio da DTIC de R\$ 1.028.293,00. Foi desconsiderado os recursos de investimento dos câmpus, não levantados até a elaboração deste documento.

Considerando que tem-se como objetivo a utilização de recurso orçamentário de três anos (2024, 2025 e 2026) a estimativa de investimento não será inferior a R\$ 3.084.879,00 (histórico 2023 e projeção para 2024).

Desta forma, não há porque limitar-se o valor do processo de aquisição ao referendado no DFD, visto que outras fontes são/serão utilizadas e para o recebimento destes recursos externos há a necessidade de processo executado.

- 3.6. O objeto da contratação também está alinhada a Estratégia de Governo Digital e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2023/2024 do Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, conforme demonstrado abaixo:

ALINHAMENTO À ESTRATÉGIA DE GOVERNO DIGITAL	
ID	Objetivos Estratégicos
Objetivo 11	Garantia da segurança das plataformas de governo digital e de missão crítica;
Objetivo 16	Otimização das infraestruturas de tecnologia da informação;

ALINHAMENTO AOS PLANOS ESTRATÉGICOS	
ID	Objetivos Estratégicos
OE.06	PETIC - Garantir infraestrutura adequada para manter e suportar as soluções de TIC (2020/2024)

ALINHAMENTO AO PDTIC 2023/2024			
ID	Ação do PDTIC	ID	Meta do PDTIC associada
Ação 3	Manter e Expandir a Infraestrutura de TIC	02	100%
		04	100%
Aquisição de equipamentos de data center (Servidores de rack e switches).			
Aquisição de equipamentos de segurança e rede sem fio (firewall/controladoras, pontos de acesso e injetores).			

4. REQUISITOS DA CONTRATAÇÃO

Requisitos de Negócio:

- 4.1. A presente contratação orienta-se pelos seguintes requisitos de negócio:
- 4.1.1. conclusão do Projeto Conecta IFSC;
 - 4.1.2. conclusão do Projeto de Ampliação da Rede de Segurança de Dados;
 - 4.1.3. proteção contra ransomware;
 - 4.1.4. ampliação da capacidade de processamento de dados.

Requisitos de Capacitação

- 4.2. As empresas vencedoras deverão capacitar as equipes de TIC para o uso correto dos equipamentos (*appliance* de backup e *firewalls*) no formato de "*hands on*".

Requisitos Legais

- 4.3. O presente processo de contratação está aderente à Constituição Federal, à Lei nº 14.133/2021, à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), ao Decreto 10.332, de 28 de abril de 2020, à Instrução Normativa SGD/ME nº 94, de 2022, Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021 e a outras legislações aplicáveis.

Requisitos Temporais

- 4.4. A empresa CONTRATADA deverá atender os prazos abaixo listados sob pena de multa por não atendimento dos mesmos:

Responsabilidade da Empresa Contratada	Tempo de Execução
Entrega dos equipamentos:	Até 120 dias corridos a partir da data de emissão da Autorização de Fornecimento de Bens;
Nova entrega dos equipamentos (quando devolvidos pela contratante por não atender às especificações solicitadas):	Até 30 dias corridos a partir da devolução/rejeição da contratante formalizada por e-mail (data de envio do e-mail);
Entrega das licenças nos locais físicos ou através de site/link para download:	Até 30 dias úteis;
Iniciar/finalizar os serviços de instalação e configuração dos equipamentos:	Até 30 dias após o recebimento dos equipamentos pelo IFSC.
Recebimento de um chamado (Garantia):	Até 1(um) dia útil a partir da abertura do chamado para dar retorno do que será realizado;
Atendimento de um chamado (Garantia):	Até 5 (cinco) dias úteis a partir da abertura de chamado pelo IFSC (desconsiderar o dia útil do

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

	item anterior) para prestar atendimento <i>onsite</i> e resolver o problema registrado;
Resolução total do problema:	A empresa terá, além dos 5 dias úteis, mais 15 dias corridos para resolver o problema apresentado caso o mesmo dependa da troca de componentes.
ATENÇÃO: 1 - Se a empresa contratada estipular um prazo maior do que 15 dias corridos (limite de 45 dias corridos) para a troca do componente, deverá deixar um equipamento com características iguais ou superiores ao equipamento retirado para manutenção. 2 - Caso a devolução do equipamento em conserto seja superior a 45 dias corridos a empresa deverá entregar um NOVO equipamento em substituição ao equipamento em conserto. Deverá ser realizado todos os procedimentos contábeis para essa substituição	

Requisitos de Segurança e Privacidade

- 4.5. Todo acesso necessário à infraestrutura de TIC será acompanhado por um servidor de TIC do IFSC.
- 4.6. A empresa contratada deverá assinar o Termo de Compromisso de Manutenção de Sigilo e o Termo de Ciência da Declaração de Manutenção de Sigilo resguardando que os recursos, dados e informações de propriedade da CONTRATANTE, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, que constituam informação privilegiada e possuem caráter de confidencialidade.

Requisitos Sociais, Ambientais e Culturais

- 4.7. Os equipamentos devem estar aderentes às seguintes diretrizes sociais, ambientais e culturais:
- 4.7.1. Ambientais:
- 4.7.1.1. Para os itens que compõem este termo de referência cuja atividade de fabricação ou industrialização seja realizada no Brasil e se enquadram no Anexo I da Instrução Normativa IBAMA nº 06, de 15/03/2013, só será admitida a oferta de produto cujo fabricante esteja regularmente registrado no Cadastro Técnico Federal de Atividades Potencialmente Poluidoras ou Utilizadoras de Recursos Ambientais, instituído pelo artigo 17, inciso II, da Lei nº 6.938, de 1981:
- 4.7.1.1.1. FTE-Categoria: Indústria de Material Elétrico, Eletrônico e Comunicações; Código: 5-2; Descrição: Fabricação de material elétrico, eletrônico e equipamentos para telecomunicação e informática.

Requisitos da Arquitetura Tecnológica

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

4.8. Os equipamentos deverão observar integralmente os requisitos de arquitetura tecnológica descritos a seguir:

4.8.1. Descrição para cada item no Quadro de Especificações Mínimas, apêndice deste termo de referência.

Requisitos de Projeto e de Implementação

4.9. Não se aplica pois não se trata de processo de desenvolvimento de software, técnicas, métodos, forma de gestão, nem documentação.

Requisitos de Implantação

4.10. Os serviços de instalação e configuração para uso dos equipamentos que compõem a solução serão fornecidos pelas empresas vencedoras conforme será detalhado no Quadro de Especificações Mínimas, apêndice deste termo de referência.

Requisitos de Garantia, Manutenção e Assistência Técnica

4.11. O prazo de garantia contratual dos bens, considerando a garantia legal, somada à garantias estendidas é de, no mínimo, 1 (um) ano para os itens 1 e 38 e 3 (três) anos para os demais itens, ou pelo prazo fornecido pelo fabricante, se superior, contado a partir do primeiro dia útil subsequente à data do recebimento definitivo do objeto.

4.12. A garantia será prestada com vistas a manter os equipamentos fornecidos em perfeitas condições de uso, sem qualquer ônus ou custo adicional para o Contratante.

4.13. A garantia abrange a realização da manutenção corretiva dos bens pelo próprio Contratado, ou, se for o caso, por meio de assistência técnica autorizada, de acordo com as normas técnicas específicas.

4.14. Entende-se por manutenção corretiva aquela destinada a corrigir os defeitos apresentados pelos bens, compreendendo a substituição de peças, a realização de ajustes, reparos e correções necessárias.

4.15. As peças que apresentarem vício ou defeito no período de vigência da garantia deverão ser substituídas por outras novas, de primeiro uso, e originais, que apresentem padrões de qualidade e desempenho iguais ou superiores aos das peças utilizadas na fabricação do equipamento.

4.16. Uma vez notificado, o Contratado deverá responder à solicitação no formato next business day (até o dia útil seguinte) e realizar a reparação ou substituição dos bens que apresentarem vício ou defeito no prazo de até 5 (cinco) dias úteis, contados a partir da data de retirada do equipamento das dependências da Administração pelo Contratado ou pela assistência técnica autorizada.

4.17. O prazo indicado no subitem anterior, durante seu transcurso, poderá ser ampliado em até 15 dias corridos para troca de componentes, mediante solicitação escrita e justificada do Contratado, aceita pelo Contratante.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 4.18. Na hipótese do período de conserto ser superior aos 15 dias corridos citados no subitem acima, o Contratado deverá disponibilizar equipamento equivalente, de especificação igual ou superior ao anteriormente fornecido, para utilização em caráter provisório pelo Contratante, de modo a garantir a continuidade dos trabalhos administrativos e acadêmicos durante a execução dos reparos.
- 4.19. Caso a devolução do equipamento em conserto seja superior a 45 dias corridos a empresa deverá entregar um NOVO equipamento em substituição ao equipamento em conserto. Deverá ser realizado todos os procedimentos contábeis para essa substituição
- 4.20. Decorrido o prazo para reparos e substituições sem o atendimento da solicitação do Contratante ou a apresentação de justificativas pelo Contratado, fica o Contratante autorizado a contratar empresa diversa para executar os reparos, ajustes ou a substituição do bem ou de seus componentes, bem como a exigir do Contratado o reembolso pelos custos respectivos, sem que tal fato acarrete a perda da garantia dos equipamentos.
- 4.21. O custo referente ao transporte dos equipamentos cobertos pela garantia será de responsabilidade do Contratado.
- 4.22. A garantia legal ou contratual do objeto tem prazo de vigência própria e desvinculado daquele fixado no contrato, permitindo eventual aplicação de penalidades em caso de descumprimento de alguma de suas condições, mesmo depois de expirada a vigência contratual.
- 4.23. O atendimento deverá ser no local não sendo aceito atendimento de balcão;
- 4.24. A CONTRATADA deverá disponibilizar suporte técnico em nível corporativo com, no mínimo, as seguintes características:
- 4.24.1. Manter central de atendimento para abertura de chamados da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 5 dias por semana por via telefônica.
- 4.24.2. A central deverá ser acionada por meio de ligação gratuita ou abertura de chamados pela internet. O atendimento deverá ser realizado em língua portuguesa.

Requisitos de Experiência Profissional

- 4.25. Os serviços de assistência técnica, suporte e garantia deverão ser prestados por técnicos devidamente capacitados nos produtos em questão, bem como com todos os recursos ferramentais necessários para a prestação dos serviços;

Requisitos de Formação da Equipe

- 4.26. Não serão exigidos requisitos de formação da equipe para a presente contratação.

Requisitos de Metodologia de Trabalho

- 4.27. O fornecimento dos equipamentos está condicionado ao recebimento pelo Contratado de Autorização de Fornecimento de Bens (AFB) emitida pela Contratante.
- 4.28. A AFB indicará o tipo de equipamento, a quantidade e a localidade na qual os equipamentos deverão ser entregues.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 4.29. O Contratado deve fornecer meios para contato e registro de ocorrências da seguinte forma: com funcionamento 24 horas por dia e 7 dias por semana de maneira eletrônica e 8 horas por dia e 5 dias por semana por via telefônica.
- 4.30. O andamento do fornecimento dos equipamentos deve ser acompanhado pelo Contratado, que dará ciência de eventuais acontecimentos à Contratante.
- 4.31. Ao finalizar os serviços de instalação e configuração a empresa vencedora deverá fornecer relatório com as atividades desenvolvidas para aceite e pagamento do IFSC;
- 4.32. Entre outras formas indicadas neste TR, a comunicação entre IFSC e as empresas vencedoras se dará por e-mail;
- 4.33. Caberá ao IFSC fornecer os ambientes tecnológicos necessários para a execução dos serviços.

Requisitos de Segurança da Informação e Privacidade

- 4.34. Os colaboradores da empresa contratada, bem como esta, deverão assinar termo de ciência e termo de manutenção do sigilo.

Requisitos de Sustentabilidade

- 4.35. Além dos critérios de sustentabilidade eventualmente inseridos na descrição do objeto, devem ser atendidos os seguintes requisitos, que se baseiam no Guia Nacional de Contratações Sustentáveis:
- 4.35.1. Deverá entregar os documentos solicitados na forma digital, com vistas a evitar ou reduzir o uso de papel e impressão, em atendimento ao Art. 9º da Política Nacional de Resíduos Sólidos (Lei nº 12.305, de 2 de agosto de 2010);
- 4.35.2. As configurações de hardware e software deverão ser realizadas visando alto desempenho com a utilização racional de energia, evitando-se a sobrecarga de equipamentos ou dispositivos elétricos e eletrônicos;
- 4.35.3. Demonstrar (mediante apresentação de catálogos, especificações, manuais, etc) que os equipamentos fornecidos, periféricos, acessórios e componentes da instalação não contém substâncias perigosas como mercúrio (Hg), chumbo (Pb), cromo hexavalente (Cr(VI)), cádmio (Cd), bifenilpolibromados (PBBs), éteres difenilpolibromados (PBDEs) em concentração acima da recomendada pela diretiva da Comunidade Econômica Européia Restriction of Certain Hazardous Substances RoHS (IN nº 1/2010 - Secretaria de Logística e Tecnologia da Informação (SLTI) do Ministério do Planejamento, Orçamento e Gestão);
- 4.35.4. Destinação Final: Todos os resíduos sólidos gerados pelos produtos fornecidos que necessitam de destinação ambientalmente adequada (incluindo embalagens vazias), deverão ter seu descarte adequado, obedecendo aos procedimentos de logística reversa, em atendimento à Lei nº 12.305/2010, que institui a Política Nacional de Resíduos Sólidos, em especial a responsabilidade compartilhada pelo ciclo de vida do produto. A empresa vencedora deverá aplicar o disposto nos Artigos de nºs 31 a 33 da Lei nº 12.305 de 02 de agosto de 2010 e nos Artigos de nºs 13 a 18 do Decreto nº 7.404 de 23 de dezembro de 2010, principalmente, no que diz respeito à Logística Reversa;

Requisitos de Capacidade Técnica

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 4.36. A licitante deverá comprovar que já forneceu os equipamentos e softwares solicitados e que tem capacidade de atender às quantidades estabelecidas no Termo de Referência.

Requisitos de Compatibilidade Técnica

- 4.37. Os equipamentos de rede sem fio e firewall deverão ser da fabricante FORTINET e o servidor tipo lâmina deverá ser da fabricante HP, pois estas compõem os serviços de redes, segurança e processamento implantados no IFSC desde 2020/2021.

Subcontratação

- 4.38. Não é admitida a subcontratação do objeto contratual.

Da verificação de amostra do objeto

- 4.39. Não será solicitada amostras do objeto a ser adquirido.

Garantia da Contratação

- 4.40. 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.

5. PAPÉIS E RESPONSABILIDADES

5.1. São obrigações da CONTRATANTE:

- 5.1.1. encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Autorização de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;
- 5.1.2. receber o objeto fornecido pelo Contratado que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;
- 5.1.3. aplicar à contratada as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;
- 5.1.4. liquidar o empenho e efetuar o pagamento à contratada, dentro dos prazos preestabelecidos em contrato;
- 5.1.5. comunicar à contratada todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.2. São obrigações do CONTRATADO:

- 5.2.1. manter, durante toda a vigência da Ata de Registro de Preços, as mesmas condições da habilitação;
- 5.2.2. efetuar a entrega dos bens em perfeitas condições, conforme especificações, prazo e local constantes no subitem 6.4 deste Termo de Referência e seus anexos, acompanhado da respectiva nota fiscal, na qual constarão as indicações referentes a: marca, fabricante, modelo, procedência e prazo de garantia ou validade.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 5.2.3. os bens deverão ser entregues acompanhados de manual do usuário, com uma versão em português ou inglês, e da relação da rede de assistência técnica autorizada.
- 5.2.4. responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com os artigos 12, 13 e 17 a 27, do Código de Defesa do Consumidor (Lei nº 8.078, de 1990).
- 5.2.5. substituir, reparar ou corrigir, às suas expensas, no prazo de **05 (cinco) dias úteis**, o objeto com avarias ou defeitos.
- 5.2.6. materiais entregues em desacordo com o Edital e não retirados em até **05 (cinco) dias úteis** após comunicação formal do IFSC, serão descartados. Este prazo poderá ser prorrogado, desde que formalizado, justificado e aceito pelo IFSC. Esta prorrogação somente será aceita caso seja feita dentro do prazo da notificação.
- 5.2.7. comunicar à Contratante, no prazo máximo de **24 (vinte e quatro) horas** que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação.
- 5.2.8. responder pelas perdas e danos causados por seus empregados, durante o fornecimento do material, ainda que involuntariamente, às instalações do prédio, máquinas, equipamentos e demais bens do IFSC, substituindo os referidos bens por outros semelhantes em prazo que lhe será expressamente combinado pela Contratante.
- 5.2.9. Retirar a nota de empenho em até 03 (três) dias úteis, após a convocação.
- 5.2.10. Cumprir o prazo de garantia de acordo com o especificado em cada item neste Termo de Referência ou conforme o prazo estabelecido na proposta de preços, caso este seja maior que o mínimo estabelecido.
- 5.2.11. Arcar com todos os custos para cumprimento da garantia, inclusive no caso de necessidade de transporte (técnicos ou equipamentos).
- 5.2.12. A Contratada assume o compromisso de receber as Autorizações de Fornecimento de Bens (AFB's) e Empenhos pelo e-mail institucional informado na DECLARAÇÃO DE CONCORDÂNCIA À ATA DE REGISTRO DE PREÇOS concordando que não sendo confirmado o recebimento do e-mail, o IFSC considerará como recebido, iniciando a contagem do prazo de entrega. A CONTRATADA assume o compromisso de avisar a CONTRATANTE quando houver mudança do e-mail.

5.3. São obrigações do órgão gerenciador do registro de preços:

- 5.3.1. efetuar o registro do licitante fornecedor e firmar a correspondente Ata de Registro de Preços;
- 5.3.2. conduzir os procedimentos relativos a eventuais renegociações de condições, produtos ou preços registrados;
- 5.3.3. definir mecanismos de comunicação com os órgãos participantes e não participantes, contendo:
 - 5.3.3.1. as formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
 - 5.3.3.2. definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável;

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

5.3.4. definir mecanismos de controle de fornecimento da solução de TIC, observando, dentre outros:

5.3.4.1. a definição da produtividade ou da capacidade mínima de fornecimento da solução de TIC;

5.3.4.2. as regras para gerenciamento da fila de fornecimento da solução de TIC aos órgãos participantes e não participantes, contendo prazos e formas de negociação e redistribuição da demanda, quando esta ultrapassar a produtividade definida ou a capacidade mínima de fornecimento e for requerida pelo contratado; e

5.3.4.3. as regras para a substituição da solução registrada na Ata de Registro de Preços, garantida a verificação de Amostra do Objeto, observado o disposto no inciso III, alínea "c", item 2 do art. 17 da Instrução Normativa SGS/ME nº 94, de 2022, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

Rotinas de Execução

Do Encaminhamento Formal de Demandas

- 6.1. O gestor administrativo da reitoria/câmpus do IFSC emitirá a autorização de fornecimento de bens (AFB) para a entrega dos bens desejados.
- 6.2. O Contratado deverá fornecer equipamentos com as mesmas configurações e quantidades definidas na AFB.
- 6.3. O recebimento provisório e definitivo dos bens é disciplinado em tópico próprio deste TR.
- 6.4. As entregas deverão ser realizadas nos seguintes endereços:

CÂMPUS	ENDEREÇO
Câmpus Araranguá	Av. XV de Novembro, s/nº – Bairro Aeroporto – CEP: 88900-000 – Araranguá – SC – Fone: (48) 3311-5000; e-mail: compras.ararangua@ifsc.edu.br .
Câmpus Caçador	Av. Fahdo Thomé, 3000, Champagnat – Caçador – SC – 89503-550, Fone: (49) 3561-5700; e-mail: compras.cdr@ifsc.edu.br .
Câmpus Canoinhas	AV. Expedicionários, 2150 – Bairro Campo do Água Verde – CEP 89460-000 – Canoinhas SC: Fone: (47) 3627-4500; e-mail: compras.canoinhas@ifsc.edu.br .
Câmpus Chapecó	Av. Nereu Ramos, 3450 D – Bairro Seminário – Chapecó/SC CEP: 89813-000 – Fone: (49) 3313-1240; e-mail: compras.chapeco@ifsc.edu.br .
Câmpus Criciúma	SC 443, km 01, nº. 845 – Bairro Vila Rica – Criciúma – SC – CEP 88813-600; Esquina com Rua Antônio Daré; Fone: (48) 3462-5000;

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

	e-mail: compras.criciuma@ifsc.edu.br .
Câmpus Florianópolis	Av. Mauro Ramos, 950 – Centro – Florianópolis/SC. CEP: 88020-300 – Almoxarifado, Fone: (48) 3211-6000; e-mail: compras.fpolis@ifsc.edu.br .
Câmpus Florianópolis-Continente	Rua 14 de Julho, 150 – Coqueiros – Florianópolis/SC – CEP: 88.075-010; Fone (48) 3877-8400; e-mail: compras.continente@ifsc.edu.br .
Câmpus Garopaba	Rua Maria Aparecida Barbosa, nº 153, Loteamento Vila de Campo – Bairro Campo Duna – Garopaba – SC – CEP 88495-000; Fone (48) 3254-7330; e-mail: compras.garopaba@ifsc.edu.br .
Câmpus Gaspar	Rua Adriano Kormann, 510 – Bairro Bela Vista – Gaspar – SC; CEP 89110-971; Fone: (47) 3318-3700; e-mail: compras.gaspar@ifsc.edu.br .
Câmpus Itajaí	Av. Vereador Abrahão João Francisco, 3899, Bairro Ressacada – Itajaí – SC; CEP 88307-303; Fone: (47) 3390-1200; e-mail: compras.itj@ifsc.edu.br .
Câmpus Jaraguá do Sul – Rau	Rua dos Imigrantes, nº 445 – Bairro Rau – 89254-430 – Jaraguá do Sul; Fone: (47) 3276-9600; e-mail: compras.rau@ifsc.edu.br
Câmpus Jaraguá do Sul	Av. Getúlio Vargas, nº 830 – Centro – Jaraguá do Sul – CEP: 89251-000, Fone: (47) 3276-8700; e-mail: compras.jar@ifsc.edu.br .
Câmpus Joinville	Rua Pavão, 1337 – Loteamento Novo Horizonte – Bairro Costa e Silva, Joinville/SC – CEP: 89220-618 – Fone: (47) 3431-5600; e-mail: compras.joinville@ifsc.edu.br .
Câmpus Lages	Rua Heitor Villa-Lobos, s/n – Bairro São Francisco – Lages – CEP 88506-400, Fone: (49) 3221-4200; e-mail: compras.lages@ifsc.edu.br .
Câmpus Palhoça-Bilíngue	Rua João Bernardino da Rosa – Bairro Cidade Universitária Pedra Branca – Palhoça – SC – CEP 88137-010; Fone: (48) 3341-9700; e-mail: compras.phb@ifsc.edu.br .
Câmpus São Carlos	Rua Aloísio Stoffell, 1271 – Jardim Alvorada – São Carlos/SC – CEP 89885-000; Fone: (49) 3325-4149; e-mail: compras.sca@ifsc.edu.br
Câmpus São José	R. José Lino Kretzer, 608 – Bairro Praia Comprida – CEP: 88103-310 São José – SC; Fones: (48) 3381-2800 e Fax: 3381-2812; e-mail: compras.sje@ifsc.edu.br
Câmpus São Lourenço do Oeste	Rua Aderbal Ramos da Silva, 496-514 – Bairro Progresso. São Lourenço do Oeste – CEP 89990 000; Fones: (049) 3344-8495; e-mail: compras.slo@ifsc.edu.br .
Câmpus São Miguel do Oeste	Rua 22 de Abril, s/n – Bairro São Luiz – São Miguel do Oeste – SC 89900-970, Fone: (49)3631-0400; e-mail: compras.smo@ifsc.edu.br .

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Câmpus Tubarão	BR 101 Sul, km 336 – Fone: (48) 3301-9101; E-mail: compras.tub@ifsc.edu.br
Câmpus Urupema	Estrada do Senadinho s/n – Centro – Urupema – SC – 88625-970, Fone: (49) 3236-3100; e-mail: compras.urupema@ifsc.edu.br.
Câmpus Xanxerê	Rua Euclides Hack, 1603 – Bairro Veneza – Xanxerê – SC – 89820-000; Fone: (49) 3441-7900; e-mail: compras.xxe@ifsc.edu.br.
Reitoria	Av. 14 de julho 150 – Coqueiros – Florianópolis – SC – CEP:88075-010 – Fones: (48) 3877-9000; e-mail: compras@ifsc.edu.br.

6.5 PARTICIPANTES EXTERNOS

01 UNIDADE ITEM 03 APPLIANCE DE BACKUP - TIPO 2	
LOCAL DE ENTREGA	ENDEREÇO
TRIBUNAL REGIONAL ELEITORAL DO MARANHÃO UASG: 070005	Sede do TRE-MA Avenida Senador Vitorino Freire, s/n ,Areinha. CEP: 65.010-917 CIDADE: São Luís/MAUF: MA

6.5.1 Ficam estabelecidas as regras constantes no DECRETO Nº 11.462, DE 31 DE MARÇO DE 2023, para fins de gerenciamento da ATA para uma unidade do ITEM 03 deste processo.

6.5.1.1 As empresas deverão atentar-se para este item, uma vez que este possui entrega distinta do Estado de Santa Catarina, bem como a empresa DEVERÁ participar para todos os itens do GRUPO.

Forma de execução e acompanhamento do contrato

Condições de Entrega

- 6.5. O prazo de entrega dos bens, licenças e execução dos serviços está descrito no item 4.4 deste TR, contados do envio da Autorização de Fornecimento do Bens e da Nota de Empenho;
- 6.6. Todos os itens constantes na AFB e nota de empenho devem ser entregues no mesmo momento, nas condições (não será aceita a entrega parcelada dos itens).
- 6.7. Caso não seja possível a entrega na data assinalada, a empresa deverá comunicar as razões respectivas com pelo menos 15 dias de antecedência para que qualquer pleito de prorrogação de prazo seja analisado, ressalvadas situações de caso fortuito e força maior.

Formas de transferência de conhecimento

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 6.8. A empresa, após a instalação e configuração dos equipamentos, deverá fornecer relatório detalhado deste serviço.
- 6.9. Para o serviço de Site Survey deverá emitir relatório com todas as informações necessárias para a instalação correta dos pontos de acesso, de acordo com as especificações encontradas no Quadro de Especificações Mínimas.
- 6.10. Para o treinamento da solução de segurança de dados deverá ser atendida as especificações encontradas no Quadro de Especificações Mínimas.

Procedimentos de transição e finalização do contrato

- 6.11. Mesmo finalizada a vigência da Ata de Registro de Preços a CONTRATADA é responsável pelo suporte e garantia dos equipamentos pelo prazo definido neste TR. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

Quantidade mínima de bens para comparação e controle

- 6.12. Cada AFB conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo de entrega, conforme definições deste TR.

Mecanismos formais de comunicação

- 6.13. São definidos como mecanismos formais de Comunicação, entre a Contratante e o Contratado, os seguintes:
- 6.13.1. Autorização de Fornecimento de Bens;
 - 6.13.2. Ofício;
 - 6.13.3. Sistema de abertura de chamados;
 - 6.13.4. E-mails.

Formas de Pagamento

- 6.14. Os critérios de medição e pagamento serão tratados em tópico próprio do Modelo de Gestão do Contrato.

7. MODELO DE GESTÃO DO CONTRATO

- 7.1. O contrato firmado visa atendimento dos prazos de entrega previstos neste Termo de Referência (item 4.4) e o cumprimento da GARANTIA e SUPORTE TÉCNICO, visto que os bens só serão aceitos após avaliação minuciosa da equipe técnica da Contratante que é a responsável por recebê-los.
- 7.2. 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.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 7.3. 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.
- 7.4. As comunicações entre o órgão ou entidade e o Contratado devem ser realizadas por escrito sempre que o ato exigir tal formalidade, admitindo-se o uso de mensagem eletrônica para esse fim.
- 7.5. O órgão ou entidade poderá convocar representante da empresa para adoção de providências que devam ser cumpridas de imediato.

Reunião Inicial

- 7.6. Após a assinatura do Contrato e a nomeação do Gestor e Fiscais do Contrato, 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 do contrato.
- 7.7. 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 até 15 (quinze) dias úteis da assinatura do Contrato, podendo ser prorrogada a critério da Contratante.
- 7.8. A pauta desta reunião observará, pelo menos:
- 7.8.1. Presença do representante legal da contratada, que apresentará o seu preposto;
 - 7.8.2. Entrega, por parte da Contratada, do Termo de Compromisso e dos Termos de Ciência;
 - 7.8.3. Esclarecimentos relativos a questões operacionais, administrativas e de gestão do contrato;
 - 7.8.4. 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;
 - 7.8.5. Apresentação das declarações/certificados do fabricante, comprovando que o produto ofertado possui a garantia solicitada neste termo de referência.

Fiscalização

- 7.9. 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

- 7.10. 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);

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 7.10.1. O fiscal técnico do contrato anotar 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](#));
- 7.10.2. Identificada qualquer inexecução 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](#));
- 7.10.3. O fiscal técnico do contrato informará ao gestor do contrato, 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](#)).
- 7.10.4. 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](#)).
- 7.10.5. 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

- 7.11. 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](#)).
- 7.11.1. 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

- 7.12. 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](#)).
- 7.13. O gestor do contrato acompanhará a manutenção das condições de habilitação do Contratado, para fins de empenho de despesa e pagamento, e anotar 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](#)).

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 7.14. 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](#)).
- 7.15. 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](#)).
- 7.16. 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](#)).
- 7.17. O fiscal técnico do contrato comunicará ao gestor do contrato, em tempo hábil, o término do contrato sob sua responsabilidade, com vistas à tempestiva renovação ou prorrogação contratual. ([Decreto nº 11.246, de 2022, art. 22, VII](#)).
- 7.18. O gestor do contrato deverá elaborar 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](#)).

Critérios de Aceitação

- 7.19. A avaliação da qualidade dos produtos entregues, para fins de aceitação, consiste na verificação dos critérios relacionados a seguir:
- 7.20. Todos os equipamentos fornecidos deverão ser novos (incluindo todas as peças e componentes presentes nos produtos), de primeiro uso (sem sinais de utilização anterior), não reconicionados e em fase de comercialização normal através dos canais de venda do fabricante no Brasil (não serão aceitos produtos end-of-life).
- 7.21. Todos os componentes do(s) equipamento(s) e respectivas funcionalidades deverão ser compatíveis entre si, sem a utilização de adaptadores, frisagens, pinturas, usinagens em geral, furações, emprego de adesivos, fitas adesivas ou quaisquer outros procedimentos não previstos nas especificações técnicas ou, ainda, com emprego de materiais inadequados ou que visem adaptar forçadamente o produto ou suas partes que sejam fisicamente ou logicamente incompatíveis.
- 7.22. Todos os componentes internos do(s) equipamento(s) deverá(ão) estar instalado(s) de forma organizada e livres de pressões ocasionados por outros componentes ou cabos, que possam causar desconexões, instabilidade, ou funcionamento inadequado.
- 7.23. O número de série de cada equipamento deve ser obrigatório e único, afixado em local visível, na parte externa do gabinete e na embalagem que o contém. Esse número deverá ser identificado pelo fabricante, como válido para o produto entregue e para as condições do mercado brasileiro no que se refere à garantia e assistência técnica no Brasil.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 7.24. Serão recusados os produtos que possuam componentes ou acessórios com sinais claros de oxidação, danos físicos, sujeira, riscos ou outro sinal de desgaste, mesmo sendo o componente ou acessório considerado como novos pelo fornecedor dos produtos.
- 7.25. Os produtos, considerando a marca e modelo apresentados na licitação, não poderão estar fora de linha comercial, considerando a data de LICITAÇÃO (abertura das propostas). Os produtos devem ser fornecidos completos e prontos para a utilização, com todos os acessórios, componentes, cabos etc.
- 7.26. Todas as licenças, referentes aos softwares e drivers solicitados, devem estar registrados para utilização do Contratante, em modo definitivo (licenças perpétuas), legalizado, não sendo admitidas versões “shareware” ou “trial”. O modelo do produto ofertado pelo licitante deverá estar em fase de produção pelo fabricante (no Brasil ou no exterior), sem previsão de encerramento de produção, até a data de entrega da proposta.
- 7.27. Só haverá o recebimento definitivo, após a análise da qualidade dos bens e/ou serviços, em face da aplicação dos critérios de aceitação, resguardando-se a Contratante o direito de não receber o OBJETO cuja qualidade seja comprovadamente baixa ou em desacordo com as especificações definidas neste Termo de Referência – situação em que poderão ser aplicadas à CONTRATADA as penalidades previstas em lei, neste Termo de Referência e no CONTRATO.

Procedimentos de Teste e Inspeção

- 7.28. Serão adotados como procedimentos de teste e inspeção, para fins de elaboração dos Termos de Recebimento Provisório e Definitivo:
- 7.28.1. Os equipamentos serão vistoriados detalhadamente sob as regras descritas no Quadro de Especificações Mínimas e neste Termo de Referência, devendo ser considerados possíveis respostas a esclarecimentos ocorridos durante a publicação do processo licitatório (Pregão Eletrônico).

Níveis Mínimos de Serviço Exigidos

- 7.29. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pelo Contratante para aferir objetivamente os resultados pretendidos com a contratação. São considerados para a presente contratação os seguintes indicadores:

IAE – INDICADOR DE ATRASO NO FORNECIMENTO DO EQUIPAMENTO		
Tópico	Descrição	
Finalidade	Medir o tempo de atraso na entrega dos bens constantes na Autorização de Fornecimento de Bens. Também será utilizado para avaliação do tempo de entrega quando o bem for devolvido pela contratante por não atender às especificações editalícias.	
Meta a cumprir	IAE <= 0	A meta definida visa garantir a entrega dos produtos e serviços constantes nas Autorizações de Fornecimento de Bens dentro do prazo previsto.
Instrumento de medição	AFB, Termo de Recebimento Provisório (TRP)	

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Forma de acompanhamento	A avaliação será feita conforme a linha de base do cronograma registrada na AFB. Será subtraída a data de entrega dos produtos da AFB (desde que o fiscal técnico reconheça aquela data, com registro em Termo de Recebimento Provisório) pela data de início da execução da AFB.
Periodicidade	Para cada Autorização de Fornecimento de Bens encerrada e com Termo de Recebimento Definitivo.
Mecanismo de Cálculo (métrica)	IAE = <u>TEX – TEST</u> Onde: IAE – Indicador de Atraso de Entrega da AFB; TEX – Tempo de Execução – corresponde ao período de execução da AFB, da sua data de início até a data de entrega dos produtos da AFB. A data de início será aquela constante na AFB; caso não esteja explícita, será o primeiro dia útil após a emissão da AFB. A data de entrega da AFB deverá ser aquela reconhecida pelo fiscal técnico, conforme critérios constantes neste Termo de Referência. Para os casos em que o fiscal técnico rejeita a entrega, o prazo de execução da AFB continua a correr, findando-se apenas quanto o Contratado entrega os produtos da AFB e haja aceitação por parte do fiscal técnico. TEST – Tempo Estimado para a execução da AFB – constante na AFB, conforme estipulado no Termo de Referência.
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.
Início de Vigência	A partir da emissão da AFB.
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAE: IAE <= 0: Pagamento integral da Autorização de Fornecimento de Bens; IAE >= 1 e < 30: Aplicar-se-á glosa de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso; IAE >= 30: Aplicar-se-á glosa de 10% sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso acrescido de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso limitado em 30% sobre o valor da Autorização de Fornecimento de Bens, bem como multa de 2% sobre o valor do contrato.

IAIE – INDICADOR DE ATRASO NA INSTALAÇÃO DO EQUIPAMENTO	
Tópico	Descrição
Finalidade	Medir o tempo de atraso na execução do serviço de instalação e configuração dos bens constantes na Autorização de Fornecimento de Bens.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Meta a cumprir	IAIE < = 0	A meta definida visa garantir a execução dos serviços de instalação/configuração dos bens constantes nas Autorizações de Fornecimento de Bens em relação ao tempo estimado para tal.
Instrumento de medição	Relatório de instalação/configuração, Tempo estimado de para a execução do serviço.	
Forma de acompanhamento	A avaliação será feita conforme o tempo estimado para a execução do serviço conforme item 4.4. Será subtraído tempo real de execução do serviço pelo tempo estimado para a execução do serviço.	
Periodicidade	Para cada relatório de instalação/configuração de equipamentos recebida.	
Mecanismo de Cálculo (métrica)	IAIE = <u>TEX – TEST</u> Onde: IAE – Indicador de Atraso de Entrega da AFB; TEX – Tempo de execução da instalação/configuração contado a partir da data do recebimento provisório do equipamento até a entrega do relatório de instalação/configuração. TEST – Tempo Estimado para a execução do serviço (30 dias corridos) a partir da data de entrega do equipamento.	
Observações	Obs1: Serão utilizados dias corridos na medição. Obs2: Os dias com expediente parcial no órgão/entidade serão considerados como dias corridos no cômputo do indicador.	
Início de Vigência	A partir da data de entrega do equipamento.	
Faixas de ajuste no pagamento e Sanções	Para valores do indicador IAIE: IAIE <= 0: Pagamento integral da Autorização de Fornecimento de Bens; IAE >= 1 e < 30: Aplicar-se-á glosa de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso; IAE >= 30: Aplicar-se-á glosa de 10% sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso acrescido de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso limitado em 30% sobre o valor da Autorização de Fornecimento de Bens, bem como multa de 2% sobre o valor do contrato.	

ICP - INDICADOR DE CHAMADOS ATENDIDOS DENTRO DO PRAZO

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Finalidade	Assegurar que os chamados estejam dentro do prazo de início e fim de atendimento
Meta a cumprir	ICP $\geq$ 95% (assegurar que os chamados sejam atendidos dentro do prazo de início e fim de atendimento)
Forma de acompanhamento	Cálculo do prazo de cada solicitação de suporte técnico em relação ao Nível de Serviço
Periodicidade	Mensalmente
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção
Mecanismo de cálculo (%)	$ICP = (QAP / QTA) \times 100$ Onde: ICP - Indicador de Suporte atendido dentro do prazo; QAP - Quantidade de chamados atendidos dentro do prazo; QTA - Quantidade total de chamados atendidos.
Início da vigência	Do primeiro ao último dia do mês anterior a medição
Sanções/ faixas de ajuste	ICP $\geq$ 85% e < 95%: Multa de 1,5% sobre o valor unitário do item adquirido pela empresa contratada; ICP $\geq$ 78% e < 85%: Multa de 3% sobre o valor unitário do item adquirido pela empresa contratada; ICP $\geq$ 72% e < 78%: Multa de 5% sobre o valor unitário do item adquirido pela empresa contratada; ICP < 72 %: Será aplicada a multa de 2% sobre o valor total do contrato.
OBSERVAÇÃO	- Serão considerados os chamados abertos/atendidos por unidade do IFSC. Não será considerado o total de chamados do IFSC. - A multa sobre o contrato abarcará TODOS os chamados abertos pela unidade, independente dos itens licitados.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

IEC - INDICADOR DE EFICÁCIA NO TRATAMENTO DE CHAMADOS, REQUISIÇÕES OU INCIDENTES	
Finalidade	Apurar a eficácia da contratada na resolução de chamados sem a necessidade de reabertura
Meta a cumprir	IEC => 98% (chamados solucionados na demanda original)
Forma de acompanhamento	Relatório mensal e inspeções de chamados por amostragem
Periodicidade	Mensalmente
Instrumento de medição	Deve ser aferido por meio de ferramentas, procedimentos de amostragem ou outros procedimentos de inspeção
Mecanismo de cálculo (%)	$IEC = ((TCF - TCR) / TCF) \times 100$ Onde: IEC - Indicador de disponibilidade dos serviços prestados; TCF - Total de chamados fechados; TCR - Total de chamados reabertos.
Início da vigência	Do primeiro ao último dia do mês anterior a medição
Sanções/ faixas de ajuste	Multa de 1% sobre o valor unitário do item adquirido pela empresa contratada para cada 1% abaixo da meta (98%), limitado a 28% sobre o valor do item. ICP < 70 %: Será aplicada a multa de 2% sobre o valor total do item adquirido pela empresa contratada.
OBSERVAÇÃO	- Serão considerados os chamados fechados/reabertos por unidade do IFSC. Não será considerado o total de chamados do IFSC. - A multa sobre o contrato abará TODOS os chamados abertos pela unidade, independente dos itens licitados.

Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

7.30. Nos casos de inadimplemento na execução do objeto, as ocorrências serão registradas pela Contratante, conforme a tabela abaixo:

Id	Ocorrência	Glosa / Sanção
1	Não prestar os esclarecimentos imediatamente, referente à execução do contrato salvo quando implicarem em indagações de caráter técnico, hipótese em que serão respondidos no prazo máximo de 16 horas úteis (2 dias)	Multa de 1 (um) % sobre o valor total do Contrato por dia útil de atraso em prestar as informações por escrito, ou por outro meio quando autorizado pela contratante, até o limite de 10 (dez) dias úteis.
		Após o limite de (10) dias úteis, aplicar-se-á multa de (10) % do valor total do Contrato.
2	Não atender ao indicador de nível de serviço IAE (Indicador de Atraso no Fornecimento do Equipamento)	IAE ≥ 1 e < 30 : Aplicar-se-á glosa de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso;
		IAE ≥ 30 : Aplicar-se-á glosa de 10% sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso acrescido de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso limitado em 30% sobre o valor da Autorização de Fornecimento de Bens, bem como multa de 2% sobre o valor do Contrato .
3	Não atender ao indicador de nível de serviço IAIE (Indicador de Atraso na Instalação do Equipamento)	IAIE ≥ 1 e < 30 : Aplicar-se-á glosa de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso;
		IAIE ≥ 30 : Aplicar-se-á glosa de 10% sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso acrescido de 0,5% por dia útil de atraso sobre o valor da Autorização de Fornecimento de Bens ou fração em atraso limitado em 30% sobre o valor da Autorização de Fornecimento de Bens, bem como multa de 2% sobre o valor do Contrato .
4	Não atender ao indicador de nível de serviço ICP (Indicador de Chamados Atendidos Dentro do Prazo)	ICP $\geq 85\%$ e $< 95\%$: Multa de 1,5% sobre o valor unitário do item arrematado pela empresa contratada;
		ICP $\geq 78\%$ e $< 85\%$: Multa de 3% sobre o valor unitário do item arrematado pela empresa contratada;
		ICP $\geq 72\%$ e $< 78\%$: Multa de 5% sobre o valor unitário do item arrematado pela empresa contratada;
		ICP $< 72\%$: Será aplicada a multa de 2% sobre o valor sobre o valor do Contrato.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

5	Não atender ao indicador de nível de serviço IEC (Indicador de Eficácia no Tratamento de Chamados, Requisições ou Incidentes)	Multa de 1% sobre o valor unitário do item arrematado pela empresa contratada para cada 1% abaixo da meta (98%), limitado a 28% sobre o valor do item. ICP < 70 %: Será aplicada a multa de 2% sobre o valor sobre o valor do Contrato.
6	Recusa injustificada da licitante adjudicatária em assinar a Ata de Registro de Preço ou deixar de apresentar os documentos exigidos, nos prazos e condições estabelecidas neste Edital	Multa de 10% (dez por cento) sobre o valor total da Proposta de preços vencedora
7	Rescisão do contrato por ato unilateral da administração, motivado por culpa da Contratada, garantida prévia defesa, independente das demais sanções cabíveis	Multa de 10% (dez por cento) sobre o valor total da Proposta de preços vencedora
8	Inexecução total ou parcial do objeto deste contrato por parte da contratada	Suspensão de licitar e impedimento de contratar com o órgão, entidade ou unidade administrativa pela qual a Administração Pública opera e atua concretamente, pelo prazo de até dois anos; Impedimento de licitar e contratar com órgãos e entidades da União com o consequente descredenciamento no SICAF pelo prazo de até cinco anos;
9	Não cumprir qualquer outra obrigação contratual não citada nesta tabela.	Advertência. Em caso de reincidência ou configurado prejuízo aos resultados pretendidos com a contratação, aplica-se multa de 10 (dez) % do sobre o valor do Contrato.

7.31. Nos termos do art. 19, inciso III da Instrução Normativa SGD/ME nº 94, de 2022, será efetuada a retenção ou glosa no pagamento, proporcional à irregularidade verificada, sem prejuízo das sanções cabíveis, nos casos em que o Contratado:

7.31.1. não atingir os valores mínimos aceitáveis fixados nos critérios de aceitação, não produzir os resultados ou deixar de executar as atividades contratadas; ou

7.31.2. deixar de utilizar materiais e recursos humanos exigidos para fornecimento da solução de TIC, ou utilizá-los com qualidade ou quantidade inferior à demandada;

8. CRITÉRIOS DE MEDIÇÃO E DE PAGAMENTO

Recebimento do Objeto

8.1. Os bens serão recebidos provisoriamente, de forma sumária, no ato da entrega, juntamente com a nota fiscal ou instrumento de cobrança equivalente, pelo(a) responsável pelo acompanhamento e fiscalização do contrato, para efeito de posterior verificação de sua conformidade com as especificações constantes no Termo de Referência e na proposta.

8.2. Os bens poderão ser rejeitados, no todo ou em parte, inclusive antes do recebimento provisório, quando em desacordo com as especificações constantes no Termo de Referência e na proposta, devendo ser substituídos no prazo de **15 (quinze) dias**, a contar da notificação do Contratado, às suas custas, sem prejuízo da aplicação das penalidades.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 8.3. O recebimento definitivo ocorrerá no prazo de **10 (dez) dias úteis**, a contar do recebimento da nota fiscal ou instrumento de cobrança equivalente pela Administração, após a verificação da qualidade e quantidade do material e consequente aceitação mediante termo detalhado.
- 8.4. Para as 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](#), o prazo máximo para o recebimento definitivo será de até 5 (cinco) dias úteis.
- 8.5. O prazo para recebimento definitivo poderá ser excepcionalmente prorrogado, de forma justificada, por igual período, quando houver necessidade de diligências para a aferição do atendimento das exigências contratuais.
- 8.6. 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.
- 8.7. O prazo para a solução, pelo Contratado, de inconsistências na execução do objeto ou de saneamento da nota fiscal ou de instrumento de cobrança equivalente, verificadas pela Administração durante a análise prévia à liquidação de despesa, não será computado para os fins do recebimento definitivo.
- 8.8. 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

- 8.9. 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](#).
- 8.9.1. 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](#).
- 8.10. 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:
- 8.10.1. o prazo de validade;
- 8.10.2. a data da emissão;
- 8.10.3. os dados do contrato e do órgão Contratante;
- 8.10.4. o período respectivo de execução do contrato;
- 8.10.5. o valor a pagar; e
- 8.10.6. eventual destaque do valor de retenções tributárias cabíveis.
- 8.11. 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

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus ao Contratante;

- 8.12. A nota fiscal ou instrumento de cobrança equivalente deverá ser obrigatoriamente acompanhado da comprovação da regularidade fiscal, constatada por meio de consulta *on-line* ao SICAF ou, na impossibilidade de acesso ao referido Sistema, mediante consulta aos sítios eletrônicos oficiais ou à documentação mencionada no [art. 68 da Lei nº 14.133, de 2021](#).
- 8.13. A Administração deverá realizar consulta ao SICAF para: a) verificar a manutenção das condições de habilitação exigidas no edital; b) identificar possível razão que impeça a participação em licitação, no âmbito do órgão ou entidade, que implique proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas (INSTRUÇÃO NORMATIVA Nº 3, DE 26 DE ABRIL DE 2018).
- 8.14. Constatando-se, junto ao SICAF, 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.
- 8.15. 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.
- 8.16. 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.
- 8.17. 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

- 8.18. O pagamento será efetuado no prazo de até 10 (dez) dias úteis contados da finalização da liquidação da despesa, conforme seção anterior, nos termos da [Instrução Normativa SEGES/ME nº 77, de 2022](#).
- 8.19. 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 de Custo da Tecnologia da Informação (ICTI)* de correção monetária.

Forma de pagamento

- 8.20. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pelo Contratado.
- 8.21. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.
- 8.22. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.
- 8.23. Independentemente do percentual de tributo inserido na proposta, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 8.24. 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.

Cessão de crédito

- 8.25. É admitida a cessão fiduciária de direitos creditícios com instituição financeira, nos termos e de acordo com os procedimentos previstos na [Instrução Normativa SEGES/ME nº 53, de 8 de Julho de 2020](#), conforme as regras deste presente tópico.
- 8.26. As cessões de crédito não fiduciárias não serão concedidas pelo IFSC.**
- 8.27. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.
- 8.28. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte do Contratado (cedente), a celebração do aditamento de cessão de crédito e a realização dos pagamentos respectivos também se condicionam à regularidade fiscal e trabalhista do cessionário, bem como à certificação de que o cessionário não se encontra impedido de licitar e contratar com o Poder Público, conforme a legislação em vigor, ou de receber benefícios ou incentivos fiscais ou creditícios, direta ou indiretamente, conforme [o art. 12 da Lei nº 8.429, de 1992](#), tudo nos termos do [Parecer JL-01, de 18 de maio de 2020](#).
- 8.29. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratado) pela execução do objeto contratual, restando absolutamente incólumes todas as defesas e exceções ao pagamento e todas as demais cláusulas exorbitantes ao direito comum aplicáveis no regime jurídico de direito público incidente sobre os contratos administrativos, incluindo a possibilidade de pagamento em conta vinculada ou de pagamento pela efetiva comprovação do fato gerador, quando for o caso, e o desconto de multas, glosas e prejuízos causados à Administração. (INSTRUÇÃO NORMATIVA Nº 53, DE 8 DE JULHO DE 2020 e Anexos)
- 8.30. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade do Contratado.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR E REGIME DE EXECUÇÃO

Forma de seleção e critério de julgamento da proposta

- 9.1. 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.
- 9.2. *O regime de execução do contrato será por EMPREITADA POR PREÇO UNITÁRIO.*

Da Aplicação da Margem de Preferência

- 9.3. *Aplica-se a margem de preferência conforme descrito a seguir:*

Decreto nº 7.174/2010

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Art. 5º Será assegurada preferência na contratação, nos termos do disposto no art. 3º da Lei nº 8.248, de 1991, para fornecedores de bens e serviços, observada a seguinte ordem:

I - bens e serviços com tecnologia desenvolvida no País e produzidos de acordo com o Processo Produtivo Básico (PPB), na forma definida pelo Poder Executivo Federal;

II - bens e serviços com tecnologia desenvolvida no País; e

III - bens e serviços produzidos de acordo com o PPB, na forma definida pelo Poder Executivo Federal.

Parágrafo único. As microempresas e empresas de pequeno porte que atendam ao disposto nos incisos do caput terão prioridade no exercício do direito de preferência em relação às médias e grandes empresas enquadradas no mesmo inciso.

Exigências de habilitação

9.4. Para fins de habilitação, deverá o licitante comprovar os seguintes requisitos:

Habilitação jurídica

9.5. **Pessoa física:** cédula de identidade (RG) ou documento equivalente que, por força de lei, tenha validade para fins de identificação em todo o território nacional;

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

9.7. **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>;

9.8. **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;

9.9. **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](#).

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

9.11. **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

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

Habilitação fiscal, social e trabalhista

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 9.13. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;
- 9.14. 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.
- 9.15. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);
- 9.16. 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](#);
- 9.17. Prova de inscrição no cadastro de contribuintes *Estadual/Distrital* relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;
- 9.18. Prova de regularidade com a Fazenda *Estadual/Distrital* do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;
- 9.19. Caso o fornecedor seja considerado isento dos tributos *Estadual/Distrital* 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.
- 9.20. 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

- 9.21. Certidão negativa de insolvência civil expedida pelo distribuidor do domicílio ou sede do licitante, caso se trate de pessoa física, desde que admitida a sua participação na licitação (art. 5º, inciso II, alínea “c”, da Instrução Normativa Seges/ME nº 116, de 2021), ou de sociedade simples;
- 9.22. Certidão negativa de falência expedida pelo distribuidor da sede do fornecedor - Lei nº 14.133, de 2021, art. 69, caput, inciso II);
- 9.23. Balanço patrimonial, demonstração de resultado de exercício e demais demonstrações contábeis dos 2 (dois) últimos exercícios sociais, comprovando:
- 9.23.1. Índices de Liquidez Geral (LG), Liquidez Corrente (LC), e Solvência Geral (SG) superiores a 1 (um);

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

- 9.23.2. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura; e
- 9.23.3. Os documentos referidos acima limitar-se-ão ao último exercício no caso de a pessoa jurídica ter sido constituída há menos de 2 (dois) anos.
- 9.23.4. Os documentos referidos acima deverão ser exigidos com base no limite definido pela Receita Federal do Brasil para transmissão da Escrituração Contábil Digital - ECD ao Sped.
- 9.24. Caso a empresa licitante apresente resultado inferior ou igual a 1 (um) em qualquer dos índices de Liquidez Geral (LG), Solvência Geral (SG) e Liquidez Corrente (LC), será exigido para fins de habilitação *capital mínimo de 10% do valor total estimado da contratação*.
- 9.25. As empresas criadas no exercício financeiro da licitação deverão atender a todas as exigências da habilitação e poderão substituir os demonstrativos contábeis pelo balanço de abertura. (Lei nº 14.133, de 2021, art. 65, §1º).
- 9.26. O atendimento dos índices econômicos previstos neste item deverá ser atestado mediante declaração assinada por profissional habilitado da área contábil, apresentada pelo fornecedor.

Qualificação Técnica

- 9.27. Comprovação de aptidão para o fornecimento de bens similares 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.
- 9.27.1. Para fins da comprovação de que trata este subitem, os atestados deverão dizer respeito a contratos executados com as seguintes características mínimas:
- 9.27.1.1. *Comprovação de que a comercialização do objeto deste Termo de Referência é a atividade principal da licitante;*
- 9.27.1.2. Fornecedor de quantidades aproximadas (pelo menos de 50% da quantidade solicitada para cada item de equipamentos;
- 9.27.2. Será admitida, para fins de comprovação de quantitativo mínimo, a apresentação e o somatório de diferentes atestados executados de forma concomitante.
- 9.27.3. Os atestados de capacidade técnica poderão ser apresentados em nome da matriz ou da filial do fornecedor.
- 9.27.4. O fornecedor disponibilizará todas as informações necessárias à comprovação da legitimidade dos atestados, apresentando, quando solicitado pela Administração, cópia do contrato que deu suporte à contratação, endereço atual da Contratante e local em que foi executado o objeto Contratado, dentre outros documentos.

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

- 10.1. O custo estimado total da contratação é de R\$ **9.901.330,83** (nove milhões, novecentos e um mil, trezentos e trinta reais e oitenta e três centavos), conforme custos unitários apostos na tabela do item 1.1.

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

10.2. Para Registro de Preços, 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:

10.2.1. 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 do disposto na alínea “d” do inciso II do caput do art. 124 da Lei nº 14.133, de 2021;

10.2.2. em caso de criação, alteração ou extinção de quaisquer tributos ou encargos legais ou superveniência de disposições legais, com comprovada repercussão sobre os preços registrados;

10.2.3. serão reajustados os preços registrados, respeitada a contagem da anualidade e o índice previsto para a contratação;

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União.

11.2. A contratação será atendida pela seguinte dotação:

11.2.1. Gestão/Unidade: 158516;

11.2.2. Fonte de Recursos: 1000000000;

11.2.3. Programa de Trabalho: 171270;

11.2.4. Elemento de Despesa: 449052 e 339040;

11.2.5. Plano Interno: L20RLP01CTN;

11.3. A dotação relativa aos exercícios financeiros subsequentes será indicada após aprovação da Lei Orçamentária respectiva e liberação dos créditos correspondentes, mediante apostilamento.

Cronograma Físico Financeiro

Na tabela abaixo será considerado o triênio 2024 - 2026, diante da expectativa de renovação da ARP.

Evento	Prazo estimado	Valor
Aquisição do item 25 - 7 unidades	1 (uma) unidade com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 247.316,67
	6 (seis) unidades com recurso extra orçamentário (01/03/2024 a 31/12/2026).	R\$ 1.483.900,02
Aquisição do item 04 - 15 unidades	15 (quinze) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 22.661,25

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

	20 (vinte) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 30.215,00
	15 (quinze) unidades com recurso próprio (01/01/2026 a 31/12/2026).	R\$ 22.661,25
Aquisição do item 08 + 19 - 100 unidades	30 (trinta) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 221.867,70
	30 (trinta) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 221.867,70
	40 (quarenta) unidades com recurso próprio (01/01/2026 a 31/12/2026).	R\$ 295.823,60
Aquisição do item 09 + 20 - 40 unidades	10 (dez) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 124.888,20
	15 (quinze) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 187.332,30
	15 (quinze) unidades com recurso próprio (01/01/2026 a 31/12/2026);	R\$ 187.332,30
Aquisição do item 10 + 21 - 10 unidades	05 (cinco) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 67.169,80
	05 (cinco) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 67.169,80
Aquisição do item 30 + 22 - 04 unidades	02 (duas) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 69.634,94
	02 (duas) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 69.634,94
Aquisição do item 31 + 23 - 04 unidades	02 (duas) unidades com recurso próprio (01/03/2024 a 31/12/2024);	R\$ 100.527,88
	02 (duas) unidades com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 100.527,88
Aquisição do item 32 - 02 unidades	02 (duas) unidades com recurso extra orçamentário (01/03/2024 a 31/12/2024);	R\$ 328.278,76

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Aquisição do item 26 + 15 + 11 - 16 unidades	05 (cinco) unidades com recurso próprio (01/03/2024 a 31/12/2024); Itens 16 e 11 serão adquiridos com recursos dos câmpus.	R\$ 71.977,15
	05 (cinco) unidades com recurso próprio (01/01/2025 a 31/12/2025); Itens 16 e 11 serão adquiridos com recursos dos câmpus.	R\$ 71.977,15
	06 (seis) unidades com recurso próprio (01/01/2026 a 31/12/2026); Itens 16 e 11 serão adquiridos com recursos dos câmpus.	R\$ 86.372,58
Aquisição do item 27 + 16 + 12 - 05 unidades	01 (uma) unidade com recurso próprio (01/03/2024 a 31/12/2024); Itens 17 e 12 serão adquiridos com recursos dos câmpus.	R\$ 28.226,36
	02 (duas) unidades com recurso próprio (01/01/2025 a 31/12/2025); Itens 17 e 12 serão adquiridos com recursos dos câmpus.	R\$ 56.452,72
	02 (duas) unidades com recurso próprio (01/01/2026 a 31/12/2026); Itens 17 e 12 serão adquiridos com recursos dos câmpus.	R\$ 56.452,72
Aquisição do item 28 + 17 + 13 - 04 unidades	02 (duas) unidades com recurso próprio (01/01/2025 a 31/12/2025); O item 13 será adquirido com recursos dos câmpus.	R\$ 252.501,84
	02 (duas) unidades com recurso próprio (01/01/2026 a 31/12/2026); O item 13 será adquirido com recursos dos câmpus.	R\$ 252.501,84
Aquisição do item 29 + 18 + 14 - 02 unidades	01 (uma) unidade com recurso próprio (01/01/2025 a 31/12/2025);	R\$ 383.428,52

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

	O item 13 será adquirido com recursos dos câmpus.	
	01 (uma) unidade com recurso próprio (01/01/2026 a 31/12/2026); O item 13 será adquirido com recursos dos câmpus.	R\$ 383.428,52
Contratação do item 36	Execução com recurso próprio entre 01/03/2024 a 31/12/2024	R\$ 7.278,28
Aquisição do item 02 - 02 unidades	01 (uma) unidade com recurso extra orçamentário (01/01/2025 a 31/12/2025);	R\$ 630.484,09
	01 (uma) unidade com recurso extra orçamentário (01/01/2026 a 31/12/2026);	R\$ 630.484,09
Aquisição do item 03 - 02 unidades	01 (uma) unidade com recurso extra orçamentário (01/01/2025 a 31/12/2025);	R\$ 745.295,29
	01 (uma) unidade com recurso extra orçamentário (01/01/2026 a 31/12/2026);	R\$ 745.295,29
Demais itens do processo serão adquiridos de acordo com a necessidade, como transceivers e itens avulsos (telefonia).		

Previsão de investimento:

2024	2025	2026
R\$ 961.548,23 Recursos próprios	R\$ 1.441.107,85 Recursos próprios.	R\$ 1.284.572,81 Recursos próprios.
R\$ 1.812.178,78 Recursos extra orçamentário	R\$ 1.375.779,38 Recursos extra orçamentário	R\$ 1.375.779,38 Recursos extra orçamentário

12. CLASSIFICAÇÃO DE SIGILO DE DOCUMENTO

Câmara Nacional de Modelos de Licitações e Contratos da Consultoria-Geral da União - CNMLC
Atualização: maio/2023
Termo de Referência Aquisição de Bens de TIC - Licitação
Elaborado pela Secretaria de Gestão. Complementado e Uniformizado pela CNMLC
Identidade visual pela Secretaria de Gestão

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

O termo de referência não possui informações sensíveis/sigilosas, portanto não há necessidade de classificá-lo nos termos da Lei nº 12.527, de 18 de novembro de 2011.

Integrante Requisitante

Ederson Dantas Almeida
Técnico de TIC

Integrante Técnico

Evaristo Marcos de Quadros Jr
Analista de TIC

Integrante Administrativo

James Hilton Becker
Assistente em Administração

TERMO DE REFERÊNCIA – AQUISIÇÕES DE TIC - LICITAÇÃO

Autoridade Máxima da Área de TIC

[Benoni de Oliveira Pires](#)

Diretor de Tecnologia da Informação e Comunicação

Florianópolis, 21 de dezembro de 2023.

Aprovo,

Autoridade Competente

Thiago Rippel Pinheiro
Chefe do Departamento de Compras



INSTITUTO FEDERAL DE SANTA CATARINA

SISTEMA INTEGRADO DE PATRIMÔNIO, ADMINISTRAÇÃO E

CONTRATOS

EMITIDO EM 11/03/2024 09:06

QUADRO DE ESPECIFICAÇÕES MÍNIMAS

Licitação: 23292.034402/2023-70 - PE 31009/2023 - REI

Assunto: AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TI

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
NÃO ASSOCIADO(S) A LOTE/GRUPO					
1	ADAPTADOR DE TELEFONIA ANALÓGICA COM PORTAS FXS/FXO PRINCIPAIS CARACTERÍSTICAS: • Conversão analógico-digital do sinal de voz; • Compatível com o padrão SIP 2.0; • Duas portas LAN; • Fornece duas linhas SIP; • Possibilidade de registro independente por canal FXS / FXO; • Registra-se em diferentes servidores SIP; • Provisionamento automático; • Suporta T.38 e T.30; • Bypass, função que associa a porta FXO na porta FXS em caso de falta de energia; APLICAÇÕES: • Conversão de ramais analógicos em ramais SIP; • Envio de fax utilizando protocolo T.38; ----- ----- Especificações técnicas: Áudio • CODECs G.711 A-law e U-law, G.729 A/B, iLBC e Opus; • Jitter Buffer adaptativo; • VAD, CNG, cancelamento de eco; • T.30 com G.711; • T.38; Controle e monitoramento • Status via navegador Web; • Suporte SNMPv2; • Indicações visuais de status nos LEDs ; Funcionalidades • Atualização de firmware; • Interface Web para configuração; • Interface de configuração IVR; • Syslog; • SNMP; • Auto provisionamento; • Interface multiusuário; • SNMPv2; • TR069; Funcionalidades FXS / FXO • Conferência de até três interlocutores; • Música em espera; • DTMF relay - In-band, Out-band e SIP INFO; • Chamada em espera; • Mudo; • Transferência de chamadas; • Pêndulo; • Hot-line; • Identificador de chamadas; • Dial plan; • Blacklist; • Histórico de chamadas; • Roteamento avançado de chamadas; • Bloqueio de chamadas a cobrar; Protocolos • SIP 2.0 (RFC 3261, 3262, 3263, 3264); • Compatibilidade com a RFC 2543; • Session Timer (RFC 4028); • SDP (RFC 2327); • RTP/RTCP (RFC 1889 e RFC 1890); • NAPTR para SIP URI Lookup (RFC 2915); • STUN (RFC 3489); • ARP/RARP (RFC 826/903); • SNMP (RFC 2030); • DHCP/PPPoE; • PPTP/L2TP VPN; • HTTP Server para Web Management; • TFTP/HTTP/HTTPS para auto Provisioning; • DNS/DNS SRV (RFC 1706 e RFC 2782); • IPv4 e IPv6 (Cliente/Servidor); Aplicações • NAT/NAPT função roteador; • MAC clone; • DHCP servidor; • DHCP cliente; • VPN: PPTP/L2TP e OpenVPN; • PPPoE; • SIP redundante; • NAT transversal por STUN; • DMZ; • QoS com layer 3; • Detector de conflito de IP; Características físicas • Adaptador de energia: • Entrada: CA 110 ~ 220 V; • Saída: CC 12 V / 1 A; Conexões: • Três portas RJ45 de rede fast Ethernet; 10/100 Mbps (duas LANs e uma WAN); • Uma porta RJ11 FXO; • Uma porta RJ11 FXS (opera normalmente com cabo AWG de até 500 metros); • LEDs de status do equipamento; • Botão reset; • Dimensões: 120x28x80 mm; • Peso (aproximado): 140 gramas (sem embalagem); Garantia: • Garantia: 12 meses; MODELO DE REFERÊNCIA: KAP 311 - KHOMP	UNIDADE	50	928,00	46.400,00
26	SERVIDOR EM LÂMINA - HPE Synergy 480 Gen10 Plus; Modelo: HPE Synergy 480 Gen10 Plus CTO Compute Module [P22139-B21]; Processador:(02x) Intel Xeon-Silver 4316 2.3GHz 20-core 150W; Memória RAM: 768GB de Memória (12x) HPE 64GB (1x64GB) Dual Rank x4 DDR4-3200 CAS-22-22-22; Registered Smart Memory Kit; Armazenamento: (02x) HPE 480GB SATA 6G Read Intensive SFF SC Multi Vendor SSD; Controladora de Armazenamento: (01x) HPE Smart Array E208i-c SR Gen10 (8 Internal Lanes/No Cache) 12G SAS Modular Controller; Controladora de Rede: (01x) HPE Synergy 4820C 10/20/25Gb Converged Network Adapter; Diversos: (01x) HPE Synergy 480 Gen10 Plus 2SFF Standard Drive Cage Kit; Formato: Lâmina de meia altura (Half height); Sistema Operacional: VMware vSphere Enterprise Plus 5yr E-LTU; Gerenciamento: HPE Composer powered by OneView HPE iLO 5 ASIC; Garantia/ Suporte: Garantia de 05 anos On-site, com atendimento 24x7 e com um tempo de solução em 6 horas a partir da abertura do chamado; HPE 5Y TC Critical SVC. INSTALAÇÃO: A empresa vencedora deverá realizar a instalação do equipamento dentro do ambiente do IFSC (Reitoria) obedecendo as melhores práticas e orientações do fabricante. Após a instalação e configuração deverá executar o repasse de conhecimento - hands on - para os técnicos do IFSC e entregar a documentação final do projeto. TODO O MATERIAL NECESSÁRIO PARA A INSTALAÇÃO DVERÁ SER FORNECIDO PELA CONTRATADA. ----- ATENÇÃO: O Sistema Operacional VMware vSphere Enterprise Plus 5yr E-LTU DEVERÁ ser entregue junto com o servidor em quantidades suficientes	UNIDADE	7	247.316,67	1.731.216,69

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	para o bom funcionamento do mesmo, sem ônus adicionais para o IFSC. ----- CERTIFICAÇÕES E COMPATIBILIDADES Certificação VmWare - O modelo do servidor ofertado deve ser totalmente compatível com o software de virtualização VmWare, na versão mínima vSphere 6 ou superior, através de pesquisa ao link: http://www.vmware.com/resources/compatibility/search.php Os servidores devem estar na lista de hardware homologado Vmware vSAN https://www.vmware.com/resources/compatibility/search.php?deviceCategory=vsan Certificação RedHat - O modelo do servidor ofertado deve constar na lista de equipamentos certificados pela Red Hat, possuindo o Red Hat Hardware Catalog no mínimo na versão 6 ou superior, a pesquisa poderá ser feita através do link: http://hardware.redhat.com/hcl/ Certificação Suse - O modelo do servidor ofertado deve constar na lista de equipamentos certificados pela Novell Suse, possuindo certificação para no mínimo a versão enterprise 11 ou superior, a pesquisa poderá ser feita através do link: http://developer.novell.com/yessearch/Search.jsp Certificação Microsoft - O modelo do servidor ofertado deve constar na lista de equipamentos que possuem Certified Servers for Windows Server 2012 ou superior do Windows Server Catalog, através de pesquisa ao link: http://www.windowsservercatalog.com O SERVIDOR deve estar em conformidade com a norma IEC 60950 ou 17050-1 (Safety of Information Technology Equipment Including Electrical Business Equipment), para segurança do usuário contra incidentes elétricos e combustão dos materiais elétricos. O servidor ofertado deve possuir certificado e estar em conformidade com as normas CISPR22 ou EN55024, para assegurar níveis de emissão eletromagnética. Os equipamentos ofertados devem estar em conformidade com o padrão RoHS (Restriction of Hazardous Substances), isto é, deve ser construído com materiais que não agredem o meio ambiente. O fabricante deve possuir comprovadamente certificação ISO 14001 – Gestão Ambiental; SERVIÇO DE SUPORTE E GARANTIA A Manutenção Corretiva de Hardware e Software deverá ser prestada 7 dias por semana, 24 horas por dia, inclusive feriados. A Central de Atendimento da Assistência Técnica indicada pela CONTRATADA ou fabricante deverá estar disponível para a abertura de chamados técnicos de hardware e de software durante 7 dias por semana, 24 horas por dia, inclusive feriados. A Central de Atendimento deverá permitir discagem gratuita (0800) ou qualquer outro meio de acesso de disponibilidade imediata, sem ônus para a CONTRATANTE. Para problemas técnicos que não podem ser resolvidos rapidamente de forma remota, a mesma deverá enviar um técnico nas dependências da CONTRATANTE para fornecer suporte técnico aos produtos de hardware cobertos e devolvê-los à condição operacional. Em todas as atividades de assistência técnica ou suporte, os técnicos da Contratada deverão empregar a Língua Portuguesa, exceto no uso de termos técnicos e na utilização de textos técnicos, que poderão estar redigidos em Língua Inglesa. A CONTRATADA ou fabricante deverá disponibilizar, sem custo para a CONTRATANTE, ferramenta própria, isto é, que tenha sido desenvolvida pelo fabricante do equipamento para recebimento dos eventos monitorados e para agilizar os atendimentos proativos e reativos necessários. A CONTRATADA ou fabricante deverá comprovar que presta suporte com atividades registradas neste Termo/Especificação com o objetivo de garantir e validar o suporte a ser prestado. A CONTRATADA ou fabricante deverá garantir o sigilo e a inviolabilidade das informações a que eventualmente possa ter acesso durante os procedimentos de instalação e manutenção dos equipamentos ofertados. Todos os produtos contemplados neste item devem atender aos seguintes requisitos gerais, cabendo ao licitante prover: Garantia de 60 meses on-site 24x7 com tempo de solução de 6 horas, contado a partir do registro do chamado de Hardware. O tempo de solução para resolução de problemas deverá ser do fabricante dos equipamentos, devendo o mesmo ser comprovado através de documentação e contemplado na proposta. Não deverá haver qualquer limitação para o número de solicitações de suporte de software ou de hardware. Site na WEB (indicar endereço) com as seguintes funcionalidades: Registro e notificações automáticas de eventos dos equipamentos ofertados; Suporte on-line; Opção para personalização das informações de suporte técnico; Capacidade de organizar, compartilhar e monitorar os contratos e garantias vigentes; Criação de relatórios sob demanda; Serviço de Atendimento 24x7 através de linha telefônica 0800 do licitante (indicar na proposta) para abertura e gerenciamento de chamados técnicos e suporte de Software. A contratada deverá ainda disponibilizar atendimento telefônico para esclarecimento de dúvidas, apoio em configurações e prover orientações quanto ao uso e boas práticas de configuração da solução. Tal atendimento deverá ser realizado através de central 0800 sem ônus para a contratante, com atendimento das 08h as 18h, em dias uteis. Todo chamado não deverá ultrapassar o prazo de 4 horas de resposta, contado a partir da solicitação feita pela CONTRATANTE. A Contratante não terá limite de solicitações para esse tipo de atendimento. Atualizações devem ser realizadas pelo fornecedor no período de garantia do HARDWARE.				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	Instalação e configuração do HARDWARE sob responsabilidade do fornecedor.				
38	USER MEDIA GATEWAY - VOIP PRINCIPAIS CARACTERÍSTICAS • 4 portas de rede gigabit Ethernet; • 1 link E1/T1; • Cadastre até 10 contas SIP; • SBC – roteamento entre canais VoIP; • Sobrevivência – SAS; Especificações técnicas Especificações do link E1/T1 • 1 link E1/T1; • Permite selecionar quantidade de canais para adequar com operadora de telefonia; • Sinalização ISDN ou R2 (R2 somente para E1); • ISDN PRI; • Opções de conector;; • BNC coaxial – resistência elétrica: 75 Ohms; • RJ45 – resistência elétrica: 120 Ohms; • Configuração de clock; • Suporta método de verificação de erros (CRC-4); • Seleção de algoritmo de alocação dos canais (primeiro canal livre ou balanceado); • Ordenação de alocação dos canais; • Configurações avançadas da sinalização ISDN e R2; • Bloqueio de chamada a cobrar por duplo atendimento na sinalização R2; • Bloqueio de chamada a cobrar por sinalização no ISDN; VoIP • Criação de até 10 contas VoIP com ou sem registro; Codecs suportados: • G.711 (a-law e µ-law); • G.729A; • G.723 e G.726; • Seleção de porta de rede para protocolos SIP e RTP para cada conta VoIP; • SIP e RTP utilizando protocolo TCP; • Suporte a Keep Alive (SIP OPTIONS); • Opção de ignorar porta de origem; • Utilização do número de destino através da URI; • Relatório de causa Q.850; Seleção de modo de envio de DTMF: • In band; • Out band – RTP (RFC 2833); • Out band – SIP Info; • Suporte a fax T.38 e pass-through; Cancelamento de eco; • Filtro padrão e filtro duplo • Ajuste de tail-length até 128 ms Sobrevivência - SAS • Suporta o registro de até 120 ramais neste modo; Autorização de registro • Suporta o registro de até 120 ramais remotos; Segurança • Acesso à interface web através de senha; • Acesso através do protocolo HTTP ou HTTPS; • ACL – Lista de controle de acesso à Interface Web; • Register authorization; Roteamento • Seleção de rota por prefixo; • Seleção de rota por expressões regulares; • Modificação de número de destino e origem; • Forçar codec e perfil de destino na rota com saída VoIP; • Failover de rotas • Utilização do "Display name" como identificador de chamadas; • Cadastro de até 50 rotas • 120 ramais para autorização de registros (respeitando a tabela de recursos); Outras funcionalidades • Configuração Web simplificada; • Wizard de configuração inicial em única etapa; • Interface de diagnóstico; • Dashboard com estado dos canais e estatísticas das chamadas; • Ajuste de volume de linha; • Supressão do DTMF; • CDR personalizável; • Suporte SNMP; • Registro de logs local ou em servidor remoto; • Acesso FTP; Físico / Ambiental • Conector da fonte de energia polarizada 12 VCC; • Adaptador de energia: • Entrada: 100–240 VAC, 50/60 Hz; • Saída: 12 VCC / 2.5 A; • Consumo máximo de energia: 12 W; • 4 x RJ45 gigabit Ethernet 10/100/1000 Mbps (1 frontal, 3 traseira); • LED de status do equipamento; • LED de status do link E1/T1; • LED de alerta de erros; • Botão reset; • Dimensões aproximadas: 205 x 42 x 102 mm; • Peso aproximado: 621 g (sem embalagem); • Temperatura de operação: 0–50 °C; • Umidade de operação: 10–90% não condensado; • Temperatura de armazenamento: 0 °C a 85 °C; • Umidade de armazenamento: 10–90% não condensado; • Parafuso para aterramento direto; • Garantia: 12 meses; MODELO DE REFERÊNCIA: UMG 104 - KHOMP	UNIDADE	2	3.907,13	7.814,26
LOTE/GRUPO 1: REDE SEM FIO					
5	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA 1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia; 2. Deve permitir o fornecimento de energia capaz de alimentar os pontos de acesso deste processo 3. Deve fornecer no mínimo 30 Watts para alimentação do dispositivo com suporte PoE atendendo ao padrão IEEE 802.3at; 4. Deve acompanhar cabos de energia e acessórios para o seu perfeito funcionamento; 5. Deve ser fornecido com fonte de alimentação interna com capacidade para operar em tensões de 110V ou 220V com comutação automática. Deve acompanhar o cabo de alimentação; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).***** Deverá ser apresentado certificação do produto ofertado, caso o fabricante tenha aderido à certificação voluntária previstas na Portaria INMETRO nº 170, de 2012, ou comprovação, por qualquer meio válido, notadamente laudo pericial, de que o produto possui segurança, compatibilidade eletromagnética e eficiência energética equivalente àquela necessária para a certificação na forma da Portaria INMETRO nº 170, de 2012.	UNIDADE	50	1.510,75	75.537,50
9	PONTO DE ACESSO INDOOR - TIPO I - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Ponto de acesso (AP) apropriado para uso interno, que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança Legada da IFSC; 2. Deve permitir configuração, gerenciamento e controle pela ferramenta de gerência Fortinet (Fortigate e Fortimanager), em produção na CONTRATANTE; 3.	UNIDADE	100	6.095,48	609.548,00

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 4. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 5. Deve permitir ser gerenciado remotamente através de links WAN; 6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 15. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPSec; 17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 18. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 19. Deve permitir operação em modo Mesh; 20. Deve possuir potência de irradiação mínima de 21dBm em ambas as frequências; 21. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1200 Mbps em um único rádio; 22. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar OFDMA; 24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 25. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 26. Deve suportar BSS Coloring; 27. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 28. Deve possuir sensibilidade mínima de -94dBm quando operando em 5GHz com MCS0 (HT20); 29. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 33. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	métodos de autenticação: WPA (TKIP) e WPA2 (AES); 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 38. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 39. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 40. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 41. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 42. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 43. Deve implementar o padrão IEEE 802.11e; 44. Deve implementar o padrão IEEE 802.11h; 45. Deve implementar o padrão IEEE 802.3az; 46. Deve suportar ser gerenciado via SNMP; 47. Deve suportar consultas via REST API; 48. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 49. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C; 50. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 51. Deve possuir indicadores luminosos (LED) para indicação de status; 52. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 53. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 54. Deve possuir certificado emitido pela Wi-Fi Alliance; 55. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 56. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 57. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 58. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
10	PONTO DE ACESSO INDOOR - TIPO II - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Ponto de acesso (AP) apropriado para uso interno, que permita acesso dos dispositivos à rede através dos wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança Legada da IFSC. 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve permitir configuração, gerenciamento e controle pela ferramenta de gerência Fortinet (Fortigate e Fortimanager), em produção na CONTRATANTE; 4. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 5. Deve permitir ser gerenciado remotamente através de links WAN; 6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 10. Deve permitir a conexão de 500 (quinhentos) clientes wireless simultaneamente; 11. Deve possuir 1 (um) interface Ethernet padrão 10/100/1000Base-T com conector RJ-45 e 1 (um) interface Ethernet padrão 100/1000/2500Base-T com conector RJ-45 para permitir a conexão com a rede LAN; 12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 14. Deve permitir sua alimentação através de Power Over Ethernet (PoE) conforme os padrões 802.3af ou 802.3at. Adicionalmente deve possuir entrada de alimentação 12VDC; 15. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio	UNIDADE	40	10.293,39	411.735,60

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPsec; 17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 18. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 19. Deve permitir operação em modo Mesh; 20. Deve possuir potência de irradiação mínima de 23dBm em ambas as frequências; 21. Deve suportar, no mínimo, operação MIMO 4x4 com 4 fluxos espaciais permitindo data rates de até 1100 Mbps em um único rádio; 22. Deve suportar MU-MIMO com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar OFDMA; 24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 25. Deve suportar recurso de Target Wake Time (TWT) configurado por SSID; 26. Deve suportar BSS Coloring; 27. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 28. Deve possuir sensibilidade mínima de -90dBm quando operando em 5GHz com MCS0 (HT20); 29. Deve possuir antenas internas ao equipamento com ganho mínimo de 4dBi em 2.4GHz e 5GHz; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 32. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz; 33. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 14 (quatorze) SSIDs com operação simultânea; 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3; 38. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 39. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP; 40. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 41. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 42. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 43. Deve implementar o padrão IEEE 802.11e; 44. Deve implementar o padrão IEEE 802.11h; 45. Deve implementar o padrão IEEE 802.3az; 46. Deve suportar ser gerenciado via SNMP; 47. Deve suportar consultas via REST API; 48. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação; 49. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C; 50. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar; 51. Deve possuir indicadores luminosos (LED) para indicação de status; 52. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	processo; 53. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 54. Deve possuir certificado emitido pela Wi-Fi Alliance; 55. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 56. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 57. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 58. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
11	PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Ponto de acesso (AP) apropriado para uso externo, que permita acesso dos dispositivos à rede através do wireless e que possua todas as suas configurações centralizadas na solução de gerenciamento de redes e segurança Legada da IFSC; 2. Deve suportar modo de operação centralizado, ou seja, sua operação depende da solução de gerenciamento de redes e segurança que é responsável por gerenciar as políticas de segurança, qualidade de serviço (QoS) e monitoramento da radiofrequência; 3. Deve permitir configuração, gerenciamento e controle pela ferramenta de gerência Fortinet (Fortigate e Fortimanager), em produção na CONTRATANTE; 4. Deve identificar automaticamente a solução de gerenciamento de redes e segurança ao qual se conectará; 5. Deve permitir ser gerenciado remotamente através de links WAN; 6. Deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax de forma simultânea; 7. Deve possuir capacidade dual-band com rádios 2.4GHz e 5GHz operando simultaneamente, além de permitir configurações independentes para cada rádio; 8. O ponto de acesso deve possuir rádio Wi-Fi adicional a aqueles que conectam clientes para funcionar exclusivamente como sensor Wi-Fi com objetivo de identificar interferências e ameaças de segurança (wIDS/wIPS) em tempo real e com operação 24x7. Caso o ponto de acesso não possua rádio adicional com tal recurso, será aceita composição do ponto de acesso e hardware ou ponto de acesso adicional do mesmo fabricante para funcionamento dedicado para tal operação; 9. Deve possuir rádio BLE (Bluetooth Low Energy) integrado e interno ao equipamento; 10. Deve permitir a conexão de 400 (quatrocentos) clientes wireless simultaneamente; 11. Deve possuir 2 (duas) interfaces Ethernet padrão 10/100/1000Base-T, ou superior, com conector RJ-45 para permitir a conexão com a rede LAN; 12. Deve implementar link aggregation de acordo com o padrão IEEE 802.3ad; 13. Deve possuir interface console para gerenciamento local com conexão serial padrão RS-232 e conector RJ45 ou USB; 14. Deve permitir sua alimentação através de Power Over Ethernet (PoE). Deve acompanhar injetor PoE para alimentação do equipamento; 15. O encaminhamento de tráfego dos dispositivos conectados à rede sem fio deve ocorrer de forma centralizada através de túnel estabelecido entre o ponto de acesso e a solução de gerenciamento de redes e segurança. Neste modo todos os pacotes trafegados em um determinado SSID devem ser tunelados até a solução de gerenciamento de redes e segurança; 16. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, para garantir a integridade dos dados, este tráfego deve ser enviado pelo AP para o a solução de gerenciamento de redes e segurança através de túnel IPsec; 17. Quando o encaminhamento de tráfego dos clientes wireless for tunelado, de forma a garantir melhor utilização dos recursos, a solução deve suportar recurso conhecido como Split Tunneling a ser configurado no SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até a solução de gerenciamento de redes e segurança, ou seja, todos os pacotes devem ser tunelados exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 18. Adicionalmente, o ponto de acesso deve suportar modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser tunelados até a solução de gerenciamento de redes e segurança; 19. Deve permitir operação em modo Mesh; 20. Deve possuir potência de irradiação de 25dBm em 2.4GHz e 5GHz; 21. Deve suportar, no mínimo, operação MIMO 2x2 com 2 fluxos espaciais permitindo data rates de até 1.2 Gbps em um único rádio; 22. Deve suportar MUMIMO com operações em Downlink (DL) e Uplink (UL); 23. Deve suportar OFDMA com operações em Downlink (DL) e Uplink (UL); 24. Deve suportar modulação de até 1024 QAM para os rádios que operam em 2.4 e 5GHz servindo clientes wireless 802.11ax; 25. Deve implementar	UNIDADE	10	11.072,04	110.720,40

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	recurso de Target Wake Time (TWT) configurado por SSID; 26. Deve suportar BSS Coloring; 27. Deve suportar operação em 5GHz com canais de 20, 40 e 80MHz; 28. Deve possuir sensibilidade mínima de -91dBm quando operando em 5GHz com MCS0 (HT20); 29. Deve possuir antenas internas ao equipamento com ganho mínimo de 6dBi em 2.4GHz e 6dBi em 5GHz; 30. Em conjunto com a solução de gerenciamento de redes e segurança, deve otimizar o desempenho e a cobertura wireless (RF), realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados; 31. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos nãoWiFi e que operem nas frequências de 2.4GHz ou 5GHz; 32. Deve suportar mecanismos para detecção e mitigação automática de pontos de acesso não autorizados, também conhecidos como Rogue Aps; 33. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless (wIDS/wIPS); 34. Em conjunto com a solução de gerenciamento de redes e segurança, deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível criar até 8 (oito) SSIDs com operação simultânea; 35. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 36. Em conjunto com a solução de gerenciamento de redes e segurança, deve ser compatível e implementar o método de autenticação WPA3 com 802.1X; 37. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 38. Em conjunto com a solução de gerenciamento de redes e segurança, deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários com base nos atributos fornecidos pelos servidores RADIUS; 39. Deve implementar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 40. Deve implementar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 41. Deve implementar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 42. Deve implementar o padrão IEEE 802.11e; 43. Deve implementar o padrão IEEE 802.11h; 44. Deve implementar o padrão IEEE 802.3az; 45. Deve suportar consultas SNMP diretamente no ponto de acesso; 46. Deve suportar consultas REST API diretamente no ponto de acesso; 47. Deve possuir estrutura robusta para operação em ambientes externos e permitir ser instalado em paredes e postes. Deve acompanhar os acessórios para fixação em paredes e postes; 48. Deve ser capaz de operar em ambientes com temperaturas entre -10 e 60° C; 49. O equipamento deve possuir grau de proteção IP67. Não serão aceitos equipamentos instalados em acessórios, por exemplo caixas herméticas, para que alcancem este grau de proteção; 50. Deve possuir indicadores luminosos (LED) para indicação de status das interfaces físicas e dos rádios WiFi; 51. O ponto de acesso deverá ser compatível e ser gerenciado pela solução de gerenciamento de redes e segurança deste processo; 52. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 53. Deve possuir certificado emitido pela Wi-Fi Alliance; 54. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 55. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 56. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 57. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
20	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO I - FC-10-PF231-247-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	100	1.300,11	130.011,00
21	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO II - FC-10-F431F-247-02- 36 1.Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	40	2.195,43	87.817,20

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
22	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT OUTDOOR - FC-10-P234F-247-02- 36 1.Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	10	2.361,56	23.615,60
25	SERVIÇO TÉCNICO PARA SITE SURVEY - SOLUÇÃO DE SEGURANÇA DE DADOS 1. O serviço de Site Survey será utilizado para análise técnica do ambiente real dos campus do IFSC em todas as localidades do estado de Santa Catarina de forma presencial nos respectivos endereços, apoiada por ferramentas e softwares adequados, que indiquem: 1.1. O melhor posicionamento dos dispositivos pontos de acesso de rede sem fio para a maximização da cobertura do sinal de RF; 1.2. A quantidade exata de pontos de acesso a serem instalados por prédio; 1.3. Fontes e zonas de interferência; 1.4. O canal de frequência a ser utilizado por cada ponto de acesso; 1.5. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF em desenho colorido; 2. A unidade de serviço deve contemplar um campus independente da sua localidade; 3. Será de responsabilidade da CONTRATANTE a disponibilização de planta arquitetônica em CAD (*.dwg) para realização de predição teórica e confecção de as-built; 4. Será de responsabilidade da CONTRATADA os seguintes serviços abaixo: 4.1. A disponibilização de um ou mais técnicos para realização de testes em campos para determinar a melhor disposição dos pontos de acesso de rede sem fio; 4.2. Relatório técnico de vistoria resultante da predição teórica das plantas fornecidas pela CONTRATANTE com as seguintes informações: 4.2.1. As possíveis limitações físicas ou dificuldades de implementação detectadas nos locais – restrições da construção, obstáculos, etc.; 4.2.2. Melhor posicionamento dos dispositivos em cada andar das localidades visando a maximização da cobertura do sinal de RF; 4.2.3. A quantidade exata de pontos de acesso a ser instalados em cada andar e locais previstos no projeto; 4.2.4. As zonas e faixas de interferência detectadas durante o mapeamento de rádio frequência; 4.2.5. As faixas de frequência a serem utilizadas para cada ponto de acesso; 4.2.6. As áreas de cobertura e as taxas de transmissão ou faixas de nível de recepção de sinal de RF avaliados durante o mapeamento; 5. O relatório técnico deverá ser emitido com timbre da CONTRATADA e deverá conter o nome, data e assinatura do responsável técnico da CONTRATADA; 6. Todos os instrumentos/equipamentos e softwares necessários para a execução do serviço serão fornecidos pela CONTRATADA; 7. O relatório técnico de vistoria com o resultado do estudo de site survey deverá ser entregue ao analista ou técnico de TI lotados no campus em avaliação, em via impressa ou em meio digital em até 30 (trinta) dias úteis após assinatura do contrato para os itens acima citados	UNIDADE	12	9.674,02	116.088,24

Valor Total do Lote/Grupo: R\$ 1.565.073,54

LOTE/GRUPO 2: CONEXÃO DE REDE

23	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 1 - FC-10-S424I-247-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	4	6.139,86	24.559,44
24	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 2 - FC-10-W0524-247-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	4	8.863,76	35.455,04
31	SWITCH CORE - TIPO 1 – SOLUÇÃO DE SEGURANÇA DE DADOS Características Mínimas: 1.1 Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 1.2 Deve possuir 24 (vinte e quatro) slots SFP para conexão de fibras ópticas do tipo 1000Base-X operando em 1GbE; 1.3 Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 1.4 Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1.5 Deve possuir 1 (uma) interface USB; 1.6 Deve possuir capacidade de comutação de pelo menos 128 Gbps e ser capaz de encaminhar até 200 Mpps (milhões de pacotes por segundo); 1.7 Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 1.8 Deve possuir tabela MAC com suporte a 32.000 endereços; Deve operar com latência igual ou inferior à 1us (microsegundo); 1.9 Deve implementar Flow Control baseado no padrão IEEE 802.3X; 1.10 Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente; 1.11 Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 1.12 Deve suportar Multi-Chassis Link Agregation (MCLAG) ou mecanismo similar	UNIDADE	4	28.677,61	114.710,44

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica; 1.13 Deve suportar a comutação de Jumbo Frames; 1.14 Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 1.15 Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 1.16 Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 1.17 Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos; 1.18 Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.19 Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.20 Deve implementar serviço de DHCP Server e DHCP Relay; 1.21 Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos; 1.22 Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 1.23 Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN; 1.24 Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 1.25 Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 1.26 Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 1.27 Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 1.28 Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 1.29 Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 1.30 Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 1.31 Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 1.32 Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 1.33 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 1.34 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 1.35 Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 1.36 Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 1.37 Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados; 1.38 Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 1.39 Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 1.40 Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 1.41 Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 1.42 Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 1.43 Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 1.44 Deve suportar MAC Authentication Bypass (MAB); 1.45 Deve implementar RADIUS CoA (Change of Authorization); 1.46 Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 1.47 Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	habilitado de forma a não causar indisponibilidade da rede; 1.48 Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 1.49 Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 1.50 Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 1.51 Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 1.52 Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 1.53 Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 1.54 Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 1.55 Deve ser capaz de autorizar a transmissão de pacotes nas interfaces somente para aqueles endereços IP que foram aprendidos dinamicamente através de DHCP Snooping. Os pacotes originados por endereços IP desconhecidos deverão ser descartados; 1.56 Deve suportar o protocolo PTP (Precision Time Protocol); 1.57 Deve implementar Netflow, sFlow ou similar; 1.58 Deve suportar o envio de mensagens de log para servidores externos através de syslog; 1.59 Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 1.60 Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 1.61 Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 1.62 Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 1.63 Deve permitir ser gerenciado através de IPv6; 1.64 Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 1.65 Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 1.66 Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 1.67 Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 1.68 Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 1.69 Deverá suportar ser configurado e monitorado através de REST API; 1.70 Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark; 1.71 Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 1.72 Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 1.73 Deve suportar temperatura de operação de até 45º Celsius; 1.74 Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 1.75 Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 1.76 Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;				
32	SWITCH CORE - Tipo 2 - SOLUÇÃO DE SEGURANÇA DE DADOS Características Mínimas: 1.01 Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 1.02 Deve possuir 24 (vinte e quatro) interfaces do tipo 1000Base-T para conexão de cabos de par metálico UTP com conector RJ-45. Deve implementar a auto-negociação de velocidade e duplex destas interfaces, além de negociar automaticamente a conexão de cabos crossover (MDI/MDI-X); 1.03 Adicionalmente, deve possuir 4 (quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 1.04 Adicionalmente, deve possuir 2 (duas) slots QSFP+ para conexão de fibras ópticas do tipo 40GBase-X operando em 1GbE e 10GbE. Estas interfaces não devem ser do tipo combo e devem operar simultaneamente em conjunto com as interfaces do item anterior; 1.05 Deve possuir porta console para acesso à interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1.06 Deve possuir 1 (uma) interface USB; 1.07 Deve possuir capacidade de comutação de pelo menos 288 Gbps e ser capaz de encaminhar até 428 Mpps (milhões de pacotes por segundo); 1.08 Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 1.09 Deve possuir tabela MAC com suporte a 36.000 endereços; 1.10 Deve operar com latência igual ou inferior à 2us	UNIDADE	4	41.400,18	165.600,72

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	(microsegundo); 1.11 Deve implementar Flow Control baseado no padrão IEEE 802.3X; 1.12 Em conjunto com o Flow Control (IEEE 802.3x) o switch deverá, ao invés de enviar pause frames, definir um limite de banda que poderá ser recebida na interface quando o buffer estiver cheio. O switch deverá medir o volume de utilização do buffer para que o recebimento seja restaurado à capacidade máxima automaticamente; 1.13 Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 1.14 Deve suportar Multi-Chassis Link Aggregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica; 1.15 Deve suportar a comutação de Jumbo Frames; 1.16 Deve identificar automaticamente telefones IP que estejam conectados e associá-los automaticamente a VLAN de voz; 1.17 Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 1.18 Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 1.19 Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIPv1, RIPv2, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos; 1.20 Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.21 Deverá suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.22 Deve implementar serviço de DHCP Server e DHCP Relay; 1.23 Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos; 1.24 Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 1.25 Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN; 1.26 Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 15 (quinze) instâncias de Multiple Spanning Tree; 1.27 Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 1.28 Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 1.29 Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 1.30 Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 1.31 Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 1.32 Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 1.33 Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 1.34 Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 1.35 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de serviço do frame ethernet (IEEE 802.1p CoS); 1.36 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 1.37 Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 1.38 Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 1.39 Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados; 1.40 Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 1.41 Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 1.42 Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 1.43 Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 1.44 Deve suportar a autenticação IEEE 802.1X de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	múltiplos dispositivos em cada por porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 1.45 Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 1.46 Deve suportar MAC Authentication Bypass (MAB); 1.47 Deve implementar RADIUS CoA (Change of Authorization); 1.48 Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 1.49 Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 1.50 Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 1.51 Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 1.52 Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 1.53 Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 1.54 Deve permitir configurar o número máximo de endereços MAC que podem ser aprendidos em uma determinada porta. Caso o número máximo seja excedido, o switch deverá gerar um log de evento para notificar o problema; 1.55 Deve permitir a customização do tempo em segundos em que um determinado MAC Address aprendido dinamicamente ficará armazenado na tabela de endereços MAC (MAC Table); 1.56 Deve ser capaz de gerar log de eventos quando um novo endereço MAC Address for aprendido dinamicamente nas interfaces, quando o MAC Address mover entre interfaces do mesmo switch e quando o MAC Address for removido da interface; 1.57 Deve ser capaz de autorizar a transmissão de pacotes nas interfaces somente para aqueles endereços IP que foram aprendidos dinamicamente através de DHCP Snooping. Os pacotes originados por endereços IP desconhecidos deverão ser descartados; 1.58 Deve suportar o protocolo PTP (Precision Time Protocol); 1.59 Deve implementar Netflow, sFlow ou similar; 1.60 Deve suportar o envio de mensagens de log para servidores externos através de syslog; 1.61 Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 1.62 Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 1.63 Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 1.64 Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 1.65 Deve permitir ser gerenciado através de IPv6; 1.66 Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 1.67 Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 1.68 Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 1.69 Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 1.70 Deverá ser capaz de executar testes nas interfaces para identificar problemas físicos nos cabos de par trançado (UTP) conectados ao switch. Deverá executar os testes em todos os pares do cabo, informar o resultado do teste para cada par do cabo, além de informar a distância total do cabo; 1.71 Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 1.72 Deverá suportar ser configurado e monitorado através de REST API; 1.73 Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark; 1.74 Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 1.75 Deve suportar o padrão IEEE 802.3az (Energy Efficient Ethernet - EEE); 1.76 Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 1.77 Deve suportar temperatura de operação de até 45º Celsius; 1.78 Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 1.79 Deve ser fornecido com fontes de alimentação redundantes e internas ao equipamento, com capacidade para operar em tensões de 110V e 220V; 1.80 Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos;				
33	SWITCH CORE TIPO 3 – SOLUÇÃO DE SEGURANÇA DE DADOS Características Mínimas: 1.01 Equipamento do tipo comutador de rede ethernet com capacidade de operação em camada 3 do modelo OSI; 1.02 Deve possuir 24 (vinte e quatro) slots SFP+ para conexão de fibras ópticas do tipo 10GBase-X operando em 1GbE e 10GbE; 1.03 Adicionalmente, deve possuir ao menos 2 (dois) slots QSFP28 para conexão de fibras ópticas operando com velocidades de 40 e 100 Gigabit Ethernet; 1.04 Deve possuir porta console para acesso à	UNIDADE	2	164.139,38	328.278,76

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	interface de linha de comando (CLI) do equipamento através de conexão serial. O cabo e eventuais adaptadores necessários para acesso à porta console deverão ser fornecidos; 1.05 Deve possuir interface dedicada para gerenciamento local do tipo "out-of-band". Esta interface de gerenciamento deverá possuir porta 1000Base-T com conector RJ-45; 1.06 Deve possuir capacidade de comutação de pelo menos 880 Gbps e ser capaz de encaminhar até 1200 Mpps (Milhões de pacotes por segundo); 1.07 Deve suportar 4000 (quatro mil) VLANs de acordo com o padrão IEEE 802.1Q; 1.08 Deve suportar Q-in-Q, recurso também conhecido como Stacked VLAN ou VLAN sobre VLAN em que é possível configurar duas TAGs de VLAN no mesmo frame conforme padrão IEEE 802.1ad; 1.09 Deve possuir tabela MAC com suporte a 60.000 endereços; 1.10 Deve implementar Flow Control baseado no padrão IEEE 802.3X; 1.11 Deve suportar o padrão IEEE 802.1Qbb (Priority-based Flow Control); 1.12 Deve permitir a configuração de links agrupados virtualmente (link aggregation) de acordo com o padrão IEEE 802.3ad (Link Aggregation Control Protocol – LACP); 1.13 Deve suportar Multi-Chassis Link Aggregation (MCLAG) ou mecanismo similar para agrupar suas interfaces com interfaces de outro switch de mesmo modelo de tal forma que equipamentos terceiros reconheçam as interfaces de ambos switches como uma única interface lógica; 1.14 Deve suportar a comutação de Jumbo Frames; 1.15 Deve implementar roteamento (camada 3 do modelo OSI) entre as VLANs; 1.16 Deve suportar a criação de rotas estáticas em IPv4 e IPv6; 1.17 Deve possuir hardware capaz de suportar roteamento dinâmico através dos protocolos RIP, BGP, OSPF em IPv4 e OSPF em IPv6. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos; 1.18 Deve possuir hardware capaz de suportar roteamento multicast através do protocolo PIM-SSM (Protocol Independent Multicast - Source-Specific Multicast). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação dos protocolos; 1.19 Deve possuir hardware capaz de suportar o protocolo VRRP ou mecanismo similar de redundância de gateway. É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.20 Deve suportar Bidirectional Forwarding Detection (BFD). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação do protocolo; 1.21 Deve ser capaz de criar múltiplas tabelas de roteamento através de VRF (Virtual Routing and Forwarding). É facultada a entrega de licenças caso o software exija licenciamento adicional para ativação deste recurso; 1.22 Deve permitir configurar determinadas portas físicas do switch como interfaces de camada 3 que tenha suporte às funções de roteamento sem requerer a configuração de uma VLAN; 1.23 Deve implementar serviço de DHCP Server e DHCP Relay; 1.24 Deve suportar o protocolo Virtual Extensible LAN (VXLAN) para permitir que o tráfego de camada 2 seja encaminhado para outros locais da rede via roteamento; 1.25 Deve suportar IGMP snooping para controle de tráfego de multicast, permitindo a criação de pelo menos 1000 (mil) grupos; 1.26 Deve suportar o protocolo Multicast Listener Discovery (MLD) Snooping para otimizar as comunicações multicast em IPv6; 1.27 Deve permitir o espelhamento do tráfego de uma porta para outra porta do mesmo switch e outro switch da rede (port mirroring / SPAN); 1.28 Deve permitir o espelhamento de uma porta ou de um grupo de portas para uma porta especificada em outro equipamento através de RSPAN e ERSPAN; 1.29 Deve implementar Spanning Tree conforme os padrões IEEE 802.1w (Rapid Spanning Tree) e IEEE 802.1s (Multiple Spanning Tree). Deve implementar pelo menos 30 (trinta) instâncias de Multiple Spanning Tree; 1.30 Deve implementar recurso conhecido como PortFast ou Edge Port para que uma porta de acesso seja colocada imediatamente no status "Forwarding" do Spanning Tree após sua conexão física; 1.31 Deve implementar mecanismo de proteção da "root bridge" do algoritmo Spanning-Tree para prover defesa contra ataques do tipo "Denial of Service" no ambiente nível 2; 1.32 Deve permitir a suspensão de recebimento de BPDUs (Bridge Protocol Data Units) caso a porta esteja colocada no modo "fast forwarding" (conforme previsto no padrão IEEE 802.1w). Sendo recebido um BPDU neste tipo de porta deve ser possível desabilitá-la automaticamente; 1.33 Deve possuir mecanismo conhecido como Loop Guard para identificação de loops na rede. Deve desativar a interface e gerar um evento quando um loop for identificado; 1.34 Deve possuir mecanismo para identificar interfaces em constantes mudanças de status de operação (flapping) que podem ocasionar instabilidade na rede. O switch deverá desativar a interface automaticamente caso o número de variações de status esteja acima do limite configurado para o período estabelecido em segundos; 1.35 Deverá possuir controle de broadcast, multicast e unicast nas portas do switch. Quando o limite for excedido, o switch deve descartar os pacotes ou aplicar rate limit; 1.36 Deve suportar a criação de listas de acesso (ACLs) para filtragem de tráfego. Estas devem estar baseadas nos seguintes parâmetros para classificação do tráfego: endereço IP de origem e destino, endereço MAC de origem e destino, portas TCP e UDP, campo DSCP, campo CoS e VLAN ID; 1.37 Deve permitir a definição de dias e horários que a ACL deverá ser aplicada na rede; 1.38 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores de classe de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	serviço do frame ethernet (IEEE 802.1p CoS); 1.39 Deverá implementar classificação, marcação e priorização de tráfego baseada nos valores do campo "Differentiated Services Code Point" (DSCP) do cabeçalho IP, conforme definições do IETF; 1.40 Deverá implementar ao menos 1 (um) dos seguintes mecanismos de prevenção contra congestão de tráfego: Weighted Round Robin (WRR), WRED (Weighted Random Early Detection) ou Weighted Fair Queuing (WFQ); 1.41 Deve possuir ao menos 8 (oito) filas de priorização (QoS) por porta; 1.42 Deve suportar o mecanismo Explicit Congestion Notification (ECN) para notificar o emissor que há uma congestão ocorrendo e com isso evitar que os pacotes sejam descartados; 1.43 Deve implementar mecanismo de proteção contra ataques do tipo spoofing para mensagens de IPv6 Router Advertisement; 1.44 Deverá implementar mecanismo de proteção contra ataques do tipo man-in-the-middle que utilizam o protocolo ARP; 1.45 Deve implementar DHCP Snooping em IPv4 e IPv6 para mitigar problemas com servidores DHCP que não estejam autorizados na rede; 1.46 Deve implementar controle de acesso por porta através do padrão IEEE 802.1X com assinalamento dinâmico de VLAN por usuário com base em atributos recebidos através do protocolo RADIUS; 1.47 Deve suportar a autenticação IEEE 802.1X de múltiplos dispositivos em cada porta do switch. Apenas o tráfego dos dispositivos autenticados é que devem ser comutados na porta; 1.48 Deve suportar a autenticação simultânea de, no mínimo, 15 (quinze) dispositivos em cada porta através do protocolo IEEE 802.1X; 1.49 Deve suportar MAC Authentication Bypass (MAB); 1.50 Deve implementar RADIUS CoA (Change of Authorization); 1.51 Deve possuir recurso para monitorar a disponibilidade dos servidores RADIUS; 1.52 Em caso de indisponibilidade dos servidores RADIUS, o switch deve provisionar automaticamente uma VLAN para os dispositivos conectados nas interfaces que estejam com 802.1X habilitado de forma a não causar indisponibilidade da rede; 1.53 Deve implementar Guest VLAN para aqueles usuários que não autenticaram nas interfaces em que o IEEE 802.1X estiver habilitado; 1.54 Deve ser capaz de operar em modo de monitoramento para autenticações 802.1X. Desta forma, o switch deve permitir que sejam realizados testes de autenticação nas portas sem tomar ações tal como reconfigurar a interface; 1.55 Deve ser capaz de autenticar um computador via 802.1X mesmo que este esteja conectado através de uma interface do telefone IP; 1.56 Deve suportar RADIUS Authentication e RADIUS Accounting através de IPv6; 1.57 Deve suportar MACSec para proteger e cifrar a comunicação entre switches; 1.58 Deve suportar o protocolo PTP (Precision Time Protocol); 1.59 Deve implementar Netflow, sFlow ou similar; 1.60 Deve suportar o envio de mensagens de log para servidores externos através de syslog; 1.61 Deve suportar o protocolo SNMP (Simple Network Management Protocol) nas versões v1, v2c e v3; 1.62 Deve suportar o protocolo SSH em IPv4 e IPv6 para configuração e administração remota através de CLI (Command Line Interface); 1.63 Deve suportar o protocolo HTTPS para configuração e administração remota através de interface web; 1.64 Deve permitir upload de arquivo e atualização do firmware (software) do switch através da interface web (HTTPS); 1.65 Deve permitir ser gerenciado através de IPv6; 1.66 Deve permitir a criação de perfis de usuários administrativos com diferentes níveis de permissões para administração e configuração do switch; 1.67 Deve suportar autenticação via RADIUS e TACACS+ para controle do acesso administrativo ao equipamento; 1.68 Deverá possuir mecanismo para identificar conflitos de endereços IP na rede. Caso um conflito seja identificado, o switch deverá gerar um log de evento e enviar um SNMP Trap; 1.69 Deve suportar o protocolo LLDP e LLDP-MED para descoberta automática de equipamentos na rede de acordo com o padrão IEEE 802.1ab; 1.70 Deverá suportar protocolo OpenFlow v1.3 ou tecnologia similar para configuração do equipamento através de controlador SDN; 1.71 Deverá suportar ser configurado e monitorado através de REST API; 1.72 Deve possuir ferramenta para captura de pacotes que auxiliarão na identificação de problemas na rede. Deve permitir a utilização de filtros para selecionar o tráfego que deverá ser capturado e permitir a exportação dos pacotes através de arquivo .pcap para análise em software Wireshark; 1.73 Deve ser capaz de armazenar no mínimo duas versões de firmware simultaneamente em sua memória flash; 1.74 Deve possuir LEDs que indiquem o status de atividade de cada porta, além de indicar se há alguma falha ou alarme no switch; 1.75 Deve suportar temperatura de operação de até 40° Celsius; 1.76 Deve possuir MTBF (Mean Time Between Failures) igual ou superior a 10 (dez) anos; 1.77 Deve ser fornecido com fontes de alimentação redundantes do tipo hot-swap, com capacidade para operar em tensões de 110V e 220V; 1.78 Deve permitir a sua instalação física em rack padrão 19" com altura máxima de 1U. Todos os acessórios para montagem e fixação deverão ser fornecidos; 1.79 GARANTIA E SUPORTE: Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;				
34	TRANSCEIVER 10GBASE-LR - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Transceiver SFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas de até 10	UNIDADE	20	3.377,76	67.555,20

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	kilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).				
35	TRANSCEIVER 10GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Transceiver SFP para conexão de fibras ópticas multimodo; 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas de até 300 metros; 3. Deve possuir conector LC duplex; 4. Velocidade de 10GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	20	1.196,15	23.923,00
36	TRANSCEIVER 40GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS 1. Transceiver QSFP para conexão de fibras ópticas monomodo; 2. Deve ser compatível com o padrão 40GBASE-LR para fibras ópticas de até 10 quilômetros; 3. Deve possuir conector LC duplex; 4. Velocidade de 40GBE; 5. Deve ser compatível com os switches deste processo; 6. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V - atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote).	UNIDADE	10	30.930,54	309.305,40
Valor Total do Lote/Grupo: R\$ 1.069.388,00					
LOTE/GRUPO 3: SEGURANÇA DE REDE					
4	FONTE HOT SWAPPABLE - FORTIGATE 600E Aquisição de Fonte de Alimentação (Hot Swappable) para redundância, algo essencial em operações de rede de missão crítica, aumentando a disponibilidade e o tempo de atividade da rede, deve ser compatível com o equipamento FG-600E de acordo com as características técnicas e requisitos abaixo: 1. *Características Técnicas:* - Hot Swappable: Capacidade de substituição a quente sem a necessidade de desligar o sistema. - Tensão de Alimentação: 100-240V, 50/60 Hz. - Consumo de Energia: - Médio: 129 Watts. - Máximo: 244 Watts. - Corrente (Máxima): 6A @ 100V. - Classificação de Eficiência: 80Plus Compliant.	UNIDADE	4	8.773,50	35.094,00
6	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE 60F 1. CARACTERÍSTICAS GERAIS DA SOLUÇÃO DE NGFW 1.1. O licenciamento deverá ser compatível com o equipamento do Fabricante Fortinet modelo Fortigate 60F. 1.2. O licenciamento deverá acompanhar as funcionalidades e serviços para no mínimo: 1.2.1. Controle de Aplicações 1.2.2. Proteção IPS 1.2.3. Proteção contra Ameaças Avançadas 1.2.4. Filtro Web e de Conteúdo 1.2.5. Análise de malwares modernos em nuvem do mesmo fabricante 1.2.6. SD-WAN 1.2.7. VPN site-to-site e client-to-site 1.2.8. Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7 pelo período de 36 meses. 1.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. 1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI. 1.5. FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES: 1.5.1. Deverá reconhecer, no mínimo, 2300 (duas mil e trezentas) aplicações com base na camada 7 do modelo OSI; 1.5.2. Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários; 1.5.3. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma; 1.5.4. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.5.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.5.6. Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação. 1.5.7. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory; 1.5.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP; 1.5.9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem; 1.5.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; 1.5.11. Deverá atualizar a base de assinaturas de aplicações automaticamente; 1.5.12. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.5.13. Deve ser possível a criação de grupos de aplicações baseados em características das aplicações	UNIDADE	6	12.505,08	75.030,48

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	como: Categoria da aplicação; 1.5.14. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.15. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.16. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo; 1.5.17. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.18. Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos; 1.5.19. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação e Categoria da aplicação; 1.5.20. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet. 1.5.21. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP. 1.6. FUNCIONALIDADES DE IPS: 1.6.1. Deverá permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão; 1.6.2. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente; 1.6.3. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.6.4. Deverá possuir integração à plataforma de segurança; 1.6.5. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques; 1.6.6. Deverá utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas. 1.6.7. Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego. 1.6.8. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego; 1.6.9. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep; 1.6.10. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.6.11. Implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo; 1.6.12. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento; 1.6.13. Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos; 1.6.14. Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos. 1.6.15. Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros. 1.6.16. Deve ser possível escanear e bloquear conexões a servidores de botnet. 1.6.17. Deve dispor de opção para bloquear URLs maliciosas mediante base de dados local. 1.6.18. Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS. 1.6.19. Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS. 1.6.20. Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros. 1.6.21. Deve ser possível filtrar assinaturas com base no identificador CVE. 1.6.22. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador; 1.6.23. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável. 1.6.24. Deve incluir proteção contra-ataques de negação de serviços; 1.6.25. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.7. FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS: 1.7.1. Deverá possuir funções de antivírus e anti-spyware; 1.7.2. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP; 1.7.3. Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros); 1.7.4. Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	análise baseada em assinaturas. 1.7.5. Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo; 1.7.6. Deverá permitir o bloqueio de download de arquivos por tamanho; 1.7.7. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.8. Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros. 1.7.9. Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos. 1.7.10. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.11. A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque; 1.7.12. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente; 1.7.13. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back; 1.7.14. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento; 1.8. FUNCIONALIDADES DE FILTRO WEB E CONTEÚDO: 1.8.1. Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); 1.8.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança; 1.8.3. Deverá 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, em modo de proxy transparente e explícito; 1.8.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall; 1.8.5. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 1.8.6. Deverá possuir a função de exclusão de URLs do bloqueio; 1.8.7. Deverá permitir a customização de página de bloqueio; 1.8.8. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); 1.8.9. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário. 1.8.10. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego. 1.8.11. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website. 1.8.12. Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado. 1.8.13. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos; 1.8.14. Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo. 1.8.15. Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;				
7	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-100F 1.1. O licenciamento deverá ser compatível com o equipamento do Fabricante Fortinet modelo Fortigate 100F. 1.2. O licenciamento deverá acompanhar as funcionalidades e serviços para no mínimo: 1.2.1. Controle de Aplicações 1.2.2. Proteção IPS 1.2.3. Proteção contra Ameaças Avançadas 1.2.4. Filtro Web e de Conteúdo 1.2.5. Análise de malwares modernos em nuvem do mesmo fabricante 1.2.6. SD-WAN 1.2.7. VPN site-to-site e client-to-site 1.2.8. Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7 pelo período de 36 meses. 1.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões. 1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI. 1.5. FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES: 1.5.1. Deverá reconhecer, no mínimo, 2300 (duas mil e trezentas) aplicações com base na camada 7 do modelo OSI; 1.5.2. Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários; 1.5.3. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma; 1.5.4. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.5.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas;	UNIDADE	1	42.246,77	42.246,77

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	1.5.6. Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação. 1.5.7. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory; 1.5.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP; 1.5.9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem; 1.5.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; 1.5.11. Deverá atualizar a base de assinaturas de aplicações automaticamente; 1.5.12. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.5.13. Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação; 1.5.14. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.15. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.16. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo; 1.5.17. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.18. Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos; 1.5.19. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação e Categoria da aplicação; 1.5.20. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet. 1.5.21. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP. 1.6. FUNCIONALIDADES DE IPS: 1.6.1. Deverá permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão; 1.6.2. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente; 1.6.3. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.6.4. Deverá possuir integração à plataforma de segurança; 1.6.5. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques; 1.6.6. Deverá utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas. 1.6.7. Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego. 1.6.8. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego; 1.6.9. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep; 1.6.10. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.6.11. Implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo; 1.6.12. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento; 1.6.13. Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos; 1.6.14. Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos. 1.6.15. Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros. 1.6.16. Deve ser possível escanear e bloquear conexões a servidores de botnet. 1.6.17. Deve dispor de opção para bloquear URLs maliciosas mediante base de dados local. 1.6.18. Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS. 1.6.19. Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS. 1.6.20. Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros. 1.6.21. Deve ser possível filtrar assinaturas com base no identificador CVE. 1.6.22. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador; 1.6.23. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável. 1.6.24. Deve				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	incluir proteção contra-ataques de negação de serviços; 1.6.25. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.7. FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS: 1.7.1. Deverá possuir funções de antivírus e anti-spyware; 1.7.2. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP; 1.7.3. Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros); 1.7.4. Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas. 1.7.5. Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo; 1.7.6. Deverá permitir o bloqueio de download de arquivos por tamanho; 1.7.7. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.8. Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros. 1.7.9. Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos. 1.7.10. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.11. A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque; 1.7.12. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente; 1.7.13. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back; 1.7.14. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento; 1.8. FUNCIONALIDADES DE FILTRO WEB E CONTEÚDO: 1.8.1. Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); 1.8.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança; 1.8.3. Deverá 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, em modo de proxy transparente e explícito; 1.8.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisam logar novamente na rede para navegar pelo firewall; 1.8.5. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 1.8.6. Deverá possuir a função de exclusão de URLs do bloqueio; 1.8.7. Deverá permitir a customização de página de bloqueio; 1.8.8. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); 1.8.9. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário. 1.8.10. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego. 1.8.11. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website. 1.8.12. Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado. 1.8.13. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos; 1.8.14. Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo baseado no identificador de um canal do YouTube, por exemplo. 1.8.15. Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;				
8	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-80F 1.1. O licenciamento deverá ser compatível com o equipamento do Fabricante Fortinet modelo Fortigate 80F. 1.2. O licenciamento deverá acompanhar as funcionalidades e serviços para no mínimo: 1.2.1. Controle de Aplicações 1.2.2. Proteção IPS 1.2.3. Proteção contra Ameaças Avançadas 1.2.4. Filtro Web e de Conteúdo 1.2.5. Análise de malwares modernos em nuvem do mesmo fabricante 1.2.6. SD-WAN 1.2.7. VPN site-to-site e client-to-site 1.2.8. Garantia e suporte remoto diretamente com o fabricante na modalidade de 24x7 pelo período de 36 meses. 1.3. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação	LICENÇA	5	21.545,87	107.729,35

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	de usuários e controle granular de permissões. 1.4. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7 com base no modelo OSI. 1.5. FUNCIONALIDADES DE CONTROLE DE APLICAÇÕES: 1.5.1. Deverá reconhecer, no mínimo, 2300 (duas mil e trezentas) aplicações com base na camada 7 do modelo OSI; 1.5.2. Deverá permitir o monitoramento do tráfego de aplicações sem bloqueio de acesso aos usuários; 1.5.3. Deverá ser capaz de controlar aplicações independente do protocolo e porta utilizados, identificando-as apenas pelo comportamento de tráfego da mesma; 1.5.4. Para tráfego criptografado SSL, deve de-criptografar os pacotes a fim de possibilitar a leitura do conteúdo do pacote para checagem de assinaturas de aplicações conhecidas pelo fabricante; 1.5.5. Para manter a segurança da rede eficiente, deve suportar o controle sobre aplicações desconhecidas e não somente sobre aplicações conhecidas; 1.5.6. Deve ser possível bloquear aplicações detectadas em portas não comuns para aquela determinada aplicação. 1.5.7. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do Microsoft Active Directory; 1.5.8. Deverá permitir a criação de regras para acesso/bloqueio de aplicações por grupo de usuários do serviço de diretório LDAP; 1.5.9. Deverá permitir a criação de regras para acesso/bloqueio por endereço IP de origem; 1.5.10. Permitir nativamente a criação de assinaturas personalizadas para reconhecimento de aplicações proprietárias na própria interface gráfica da solução, sem a necessidade de ação do fabricante; 1.5.11. Deverá atualizar a base de assinaturas de aplicações automaticamente; 1.5.12. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações; 1.5.13. Deve ser possível a criação de grupos de aplicações baseados em características das aplicações como: Categoria da aplicação; 1.5.14. Deve possibilitar a diferenciação de tráfegos Peer-to-Peer (BitTorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.15. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.16. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts chat e bloquear a chamada de vídeo; 1.5.17. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos; 1.5.18. Deve ser possível limitar a banda (download/upload) usada por aplicações (traffic shaping), baseado no IP de origem, usuários e grupos; 1.5.19. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: Nível de risco da aplicação e Categoria da aplicação; 1.5.20. Deve ser possível sobrescrever uma determinada ação para uma aplicação e para um filtro, sendo que os filtros devem ter a possibilidade de ser adicionados com base no comportamento da aplicação, tais como aplicações com alto consumo de banda, evasivas e com comportamento de botnet. 1.5.21. Deve ser possível editar uma aplicação associando parâmetros a serem analisados, tal como parâmetros associados a comandos na aplicação FTP. 1.6. FUNCIONALIDADES DE IPS: 1.6.1. Deverá permitir que seja definido, através de regra por IP de origem, IP destino, protocolo e porta, qual tráfego será inspecionado pelo sistema de detecção de intrusão; 1.6.2. Deverá possuir tecnologia de detecção baseada em assinaturas que sejam atualizadas automaticamente; 1.6.3. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto; 1.6.4. Deverá possuir integração à plataforma de segurança; 1.6.5. Deverá possuir capacidade de remontagem de pacotes para identificação de ataques; 1.6.6. Deverá utilizar métodos de prevenção baseados em assinaturas, decodificadores de protocolo, análise heurística (ou monitoramento comportamental), inteligência de ameaças a partir de um centro de inteligência do próprio fabricante e detecção avançada de ameaças para evitar a exploração de ameaças conhecidas e de dia zero desconhecidas. 1.6.7. Deve ser capaz de realizar inspeção de pacotes criptografados, a fim de detectar e impedir ameaças de invasores neste perfil de tráfego. 1.6.8. Deverá possuir capacidade de agrupar assinaturas para um determinado tipo de ataque, tal como agrupar todas as assinaturas relacionadas a servidores web, para que seja usado para proteção específica deste tipo de servidor e perfil de tráfego; 1.6.9. Deverá possuir capacidade de análise de tráfego para a detecção e bloqueio de anomalias, como Denial of Service (DoS) do tipo Flood, Scan, Session e Sweep; 1.6.10. Possuir assinaturas para bloqueio de ataques de buffer overflow; 1.6.11. Implementar os seguintes tipos de ações para ameaças detectadas: permitir, permitir e gerar log, bloquear, reset de conexão e bloquear IP do atacante por um intervalo de tempo; 1.6.12. Permitir ativar ou desativar as assinaturas, ou ainda, habilitar apenas em modo de monitoramento; 1.6.13. Permitir o bloqueio de programas exploradores de vulnerabilidades conhecidos; 1.6.14. Deve ser possível criar políticas baseadas no alvo do ataque, seja servidor, cliente ou ambos. 1.6.15. Deve ser possível criar políticas com base no sistema operacional envolvido em determinada tentativa de ataque, suportando, no mínimo, Windows, Linux, MacOS, Solaris, BSD, entre outros. 1.6.16. Deve ser possível escanear e bloquear conexões a servidores de botnet. 1.6.17. Deve				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	dispor de opção para bloquear URLs maliciosas mediante base de dados local. 1.6.18. Deve ser possível habilitar a opção de salvar os pacotes correspondentes a uma determinada assinatura de IPS. 1.6.19. Deve suportar a possibilidade de criar políticas baseadas em nível de severidade das assinaturas de IPS. 1.6.20. Deve suportar a possibilidade de criar políticas baseadas no perfil da aplicação, tais como Apache, IIS, DB2, MySQL, PostgreSQL, MSSQL, MS Exchange, entre outros. 1.6.21. Deve ser possível filtrar assinaturas com base no identificador CVE. 1.6.22. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE, bem como um "wildcard" do CVE para abranger mais de um identificador; 1.6.23. As assinaturas devem dispor de um resumo explicando o ataque associado, nível de severidade, impacto e uma possível recomendação, bem como deve vincular o(s) CVE(s) correspondente(s) quando aplicável. 1.6.24. Deve incluir proteção contra-ataques de negação de serviços; 1.6.25. Registrar na console de monitoramento as seguintes informações sobre ameaças identificadas: o nome da assinatura ou do ataque, aplicação, usuário, origem e o destino da comunicação, além da ação tomada pelo dispositivo; 1.7. FUNCIONALIDADES DE PROTEÇÃO CONTRA AMEAÇAS AVANÇADAS: 1.7.1. Deverá possuir funções de antivírus e anti-spyware; 1.7.2. Deverá possuir antivírus em tempo real, para ambiente de gateway Internet, integrado à plataforma de segurança para os seguintes protocolos: HTTP, SMTP, IMAP, POP3, CIFS e FTP; 1.7.3. Deverá permitir o bloqueio de malwares (adware, spyware, hijackers, keyloggers, entre outros); 1.7.4. Deve dispor de detecção baseada em aprendizado de máquina, sendo possível inspecionar e identificar funcionalidades do arquivo que possam determinar se o mesmo tem comportamento de malware, ao invés de simplesmente realizar a análise baseada em assinaturas. 1.7.5. Deverá permitir o bloqueio de download de arquivos por extensão, nome do arquivo e tipos de arquivo; 1.7.6. Deverá permitir o bloqueio de download de arquivos por tamanho; 1.7.7. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.8. Deve dispor de funcionalidade de desarme e reconstrução visando atuar em cima de arquivos Microsoft Office e PDF, mesmo no caso de o arquivo estar compactado, removendo conteúdo maliciosos como links, JavaScript, Macros, entre outros. 1.7.9. Deve ser possível criar políticas de bloqueio de malware utilizando serviços de terceiros, onde o firewall receberá uma lista de hashes maliciosos. 1.7.10. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos; 1.7.11. A solução de sandbox deve ser capaz de criar assinaturas e ainda as incluir na base de antivírus do firewall, prevenindo a reincidência do ataque; 1.7.12. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas, impedindo que esses endereços sejam acessados pelos usuários de rede novamente; 1.7.13. Dentre as análises efetuadas, a solução deve suportar antivírus, consulta na nuvem, emulação de código, sandboxing e verificação de chamada de call-back; 1.7.14. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado de sandbox. Deve ainda disponibilizar um relatório completo da análise realizada em cada arquivo submetido, o qual poderá ser baixado para auxiliar na análise forense de um evento; 1.8. FUNCIONALIDADES DE FILTRO WEB E CONTEÚDO: 1.8.1. Deverá permitir especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora); 1.8.2. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança; 1.8.3. Deverá 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, em modo de proxy transparente e explícito; 1.8.4. A identificação pela base do Active Directory deve permitir SSO, de forma que os usuários não precisem logar novamente na rede para navegar pelo firewall; 1.8.5. Deverá suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL; 1.8.6. Deverá possuir a função de exclusão de URLs do bloqueio; 1.8.7. Deverá permitir a customização de página de bloqueio; 1.8.8. Deverá permitir o bloqueio e continuação (possibilitando que o usuário acesse um site potencialmente bloqueado informando o mesmo na tela de bloqueio e possibilitando a utilização de um botão Continuar para permitir o usuário continuar acessando o site); 1.8.9. Deve dispor de funcionalidade de prevenção contra phishing de credenciais analisando quais estão sendo submetidas em sites externos, permitindo ainda bloquear ou alertar o usuário. 1.8.10. Deve possuir a possibilidade de definir uma quota diária de uso web baseado em categoria, sendo possível estipular a quota com base em, no mínimo, tempo de uso e volume de tráfego. 1.8.11. Deve ser possível bloquear tráfego HTTP POST, método utilizado para envio de informação a um determinado website. 1.8.12. Deve ser possível filtrar e remover Java applets, ActiveX e cookies do tráfego web inspecionado. 1.8.13. Deverá possuir em sua base de dados uma lista de bloqueio contendo URLs de certificados maliciosos; 1.8.14. Deve ser possível filtrar tráfego de vídeo baseado em categoria e até mesmo				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	baseado no identificador de um canal do YouTube, por exemplo. 1.8.15. Deverá permitir além do Web Proxy explícito, suportar proxy Web transparente;				
12	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3 1. O objetivo do serviço é de configurar o dispositivo no ambiente de rede da PROPONENTE de acordo com o plano a ser aprovado pela CONTRATADA. Se o plano de configuração for fornecido pelo cliente ou proveniente de terceiros indicados pelo mesmo, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano definido pelo cliente. 2. A PROPONENTE será responsável pela conexão física dos do Equipamento do item 11 FIREWALL TIPO I - VM, conforme tabela acima respeitando a quantidade adquirida em ATA. 3. As instalações, que ocorrerão em fases conforme descritas a seguir: 3.1. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 4. Fases: 4.1. Avaliação de pré-implementação 4.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 4.2. Cronograma do plano de implementação 4.2.1. Após a avaliação, o especialista designado pela contratada deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 4.3. Execução 4.3.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 4.3.2. A maior parte da implementação será realizada remotamente. Caso necessário a CONTRATADA realizará suporte no local durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 4.3.3. A contratada deverá realizar o serviço de migração das regras de firewall da solução atual para a nova solução, o serviço deve contemplar, levantamento das regras atuais, análise das regras a serem migradas, definição das regras a serem implantadas. 4.4. Monitoramento 4.4.1. Após a conclusão da implementação a CONTRATADA realizará o monitoramento Monitoramento Proativo, disponível 24x7x365. 4.4.2. O sistema de monitoramento deve realizar as seguintes medições: - Consumo de banda; - Taxa de perda de pacote; - Taxa de erro na interface; - Alta utilização de Memória e CPU; - Conexões TCP acima do normal; - Throughput agregado; - Link inoperante; - Sistema com alarmes críticos; - Temperatura do equipamento; - Problema na fonte elétrica; - Pouco espaço em disco; - Alarme na FAN;. - Sem coleta de dados via SNMP 4.5. Relatório de implementação 4.5.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 5. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 6. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 7. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 8. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 9. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 10. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação da CONTRATADA; 11. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;	UNIDADE	16	10.084,63	161.354,08
13	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4 1. O objetivo do serviço é de configurar o dispositivo no ambiente de rede da PROPONENTE de acordo com o plano a ser aprovado pela CONTRATADA. Se o plano de configuração for fornecido	UNIDADE	5	11.148,61	55.743,05

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	pelo cliente ou proveniente de terceiros indicados pelo mesmo, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano definido pelo cliente. 2. A PROPONENTE será responsável pela conexão física dos do Equipamento do item 11 FIREWALL TIPO I - VM, conforme tabela acima respeitando a quantidade adquirida em ATA. 3. As instalações, que ocorrerão em fases conforme descritas a seguir: 3.1. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 4. Fases: 4.1. Avaliação de pré-implementação 4.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 4.2. Cronograma do plano de implementação 4.2.1. Após a avaliação, o especialista designado pela contratada deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 4.3. Execução 4.3.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 4.3.2. A maior parte da implementação será realizada remotamente. Caso necessário a CONTRATADA realizará suporte no local durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 4.3.3. A contratada deverá realizar o serviço de migração das regras de firewall da solução atual para a nova solução, o serviço deve contemplar, levantamento das regras atuais, análise das regras a serem migradas, definição das regras a serem implantadas. 4.4. Monitoramento 4.4.1. Após a conclusão da implementação a CONTRATADA realizará o monitoramento Monitoramento Proativo, disponível 24x7x365. 4.4.2. O sistema de monitoramento deve realizar as seguintes medições: - Consumo de banda; - Taxa de perda de pacote; - Taxa de erro na interface; - Alta utilização de Memória e CPU; - Conexões TCP acima do normal; - Throughput agregado; - Link inoperante; - Sistema com alarmes críticos; - Temperatura do equipamento; - Problema na fonte elétrica; - Pouco espaço em disco; - Alarme na FAN;. - Sem coleta de dados via SNMP 4.5. Relatório de implementação 4.5.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 5. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 6. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 7. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 8. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 9. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 10. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação da CONTRATADA; 11. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;				
14	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5 1. O objetivo do serviço é de configurar o dispositivo no ambiente de rede da PROPONENTE de acordo com o plano a ser aprovado pela CONTRATADA. Se o plano de configuração for fornecido pelo cliente ou proveniente de terceiros indicados pelo mesmo, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano definido pelo cliente. 2. A PROPONENTE será responsável pela conexão física dos do Equipamento do item 11 FIREWALL TIPO I - VM, conforme tabela acima respeitando a quantidade adquirida em ATA. 3. As instalações, que ocorrerão em fases conforme descritas a seguir: 3.1. Este serviço deverá incluir	UNIDADE	4	11.762,52	47.050,08

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 4. Fases: 4.1. Avaliação de pré-implementação 4.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente apontadas. 4.2. Cronograma do plano de implementação 4.2.1. Após a avaliação, o especialista designado pela contratada deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 4.3. Execução 4.3.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 4.3.2. A maior parte da implementação será realizada remotamente. Caso necessário a CONTRATADA realizará suporte no local durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 4.3.3. A contratada deverá realizar o serviço de migração das regras de firewall da solução atual para a nova solução, o serviço deve contemplar, levantamento das regras atuais, análise das regras a serem migradas, definição das regras a serem implantadas. 4.4. Monitoramento 4.4.1. Após a conclusão da implementação a CONTRATADA realizará o monitoramento Monitoramento Proativo, disponível 24x7x365. 4.4.2. O sistema de monitoramento deve realizar as seguintes medições: - Consumo de banda; - Taxa de perda de pacote; - Taxa de erro na interface; - Alta utilização de Memória e CPU; - Conexões TCP acima do normal; - Throughput agregado; - Link inoperante; - Sistema com alarmes críticos; - Temperatura do equipamento; - Problema na fonte elétrica; - Pouco espaço em disco; - Alarme na FAN; - Sem coleta de dados via SNMP 4.5. Relatório de implementação 4.5.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 5. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 6. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 7. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 8. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 9. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 10. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação da CONTRATADA; 11. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;				
15	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6 1. O objetivo do serviço é de configurar o dispositivo no ambiente de rede da PROPONENTE de acordo com o plano a ser aprovado pela CONTRATADA. Se o plano de configuração for fornecido pelo cliente ou proveniente de terceiros indicados pelo mesmo, a contratada apenas garantirá que o resultado da implementação esteja alinhado com o plano definido pelo cliente. 2. A PROPONENTE será responsável pela conexão física dos do Equipamento do item 11 FIREWALL TIPO I - VM, conforme tabela acima respeitando a quantidade adquirida em ATA. 3. As instalações, que ocorrerão em fases conforme descritas a seguir: 3.1. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução, monitoramento e relatório. 4. Fases: 4.1. Avaliação de pré-implementação 4.1.1. O especialista da contratada analisará os requisitos da contratante e compreenderá as necessidades de segurança, ambiente de rede e objetivos de negócios na implementação. Além disso, o plano de rollout também será avaliado e as inadequações serão previamente	UNIDADE	2	13.716,78	27.433,56

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	apontadas. 4.2. Cronograma do plano de implementação 4.2.1. Após a avaliação, o especialista designado pela contratada deverá desenvolver o plano de implementação, incluindo o escopo da implementação, marcos e tarefas operacionais para atender aos requisitos. O plano será modificado de acordo com os requisitos da contratante, até se obter a aceitação do cliente. O escopo de implementação não deve ser alterado depois de confirmado pelo cliente. 4.3. Execução 4.3.1. A implementação deverá ser realizada de acordo com o plano aceito pela contratante anteriormente. Mudanças de plano após o aceite da fase anterior devem ser negociadas. 4.3.2. A maior parte da implementação será realizada remotamente. Caso necessário a CONTRATADA realizará suporte no local durante a implantação para acompanhar de perto o progresso e resolver quaisquer problemas que possam surgir. 4.3.3. A contratada deverá realizar o serviço de migração das regras de firewall da solução atual para a nova solução, o serviço deve contemplar, levantamento das regras atuais, análise das regras a serem migradas, definição das regras a serem implantadas. 4.4. Monitoramento 4.4.1. Após a conclusão da implementação a CONTRATADA realizará o monitoramento Monitoramento Proativo, disponível 24x7x365. 4.4.2. O sistema de monitoramento deve realizar as seguintes medições: - Consumo de banda; - Taxa de perda de pacote; - Taxa de erro na interface; - Alta utilização de Memória e CPU; - Conexões TCP acima do normal; - Throughput agregado; - Link inoperante; - Sistema com alarmes críticos; - Temperatura do equipamento; - Problema na fonte elétrica; - Pouco espaço em disco; - Alarme na FAN; - Sem coleta de dados via SNMP 4.5. Relatório de implementação 4.5.1. O Relatório de Implantação de Lançamento deverá ser entregue para resumir o procedimento de implementação e os resultados. O relatório fornecerá à contratante uma compreensão da implantação, configuração, tarefas de operação e alguns recursos dos produtos ofertados. 5. Os serviços de instalação deverão ser executados pela CONTRATADA durante o horário comercial compreendido entre 8h às 17h, de segunda à sexta-feira, devendo, eventualmente, atender a CONTRATANTE em finais de semana e feriados para atendimento ou acompanhamento de configurações que necessitem ser executadas nestes horários, cabendo à CONTRATANTE informar tais atendimentos à CONTRATADA, antecipadamente e de comum acordo entre as partes; 6. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento. 7. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial. 8. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados. 9. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento em local adequado, assim como prover o acesso remoto a console de configuração do equipamento; 10. A equipe técnica da CONTRATANTE que irá executar a instalação deverá trabalhar sob orientação e supervisão técnica do profissional responsável pela coordenação das atividades de implantação da CONTRATADA; 11. A CONTRATADA, depois de concluído o serviço de configuração dos equipamentos da solução, deverá realizar, com o acompanhamento remoto dos técnicos da CONTRATANTE, testes de pré-operação para constatar que a solução foi devidamente instalada e configurada de acordo com o cenário requerido pela CONTRATANTE; 12. Quando não aprovado o funcionamento de quaisquer itens da solução, a CONTRATADA deverá anotar no RI as ocorrências e suas origens, tomar toda e qualquer providência necessária para resolvê-las, sem gerar ônus adicional à CONTRATANTE e sem prejudicar o tempo previsto de instalação;				
16	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3 - FC-10-0080F-950-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	16	20.446,53	327.144,48
17	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4 - FC-10-F100F-950-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	5	40.091,21	200.456,05
18	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5 - FC-10-F200F-950-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	4	74.088,60	296.354,40
19	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6 - FC-10-F6H0E-950-02-36 1. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis;	UNIDADE	2	202.947,00	405.894,00
27	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 3 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada	UNIDADE	16	14.395,43	230.326,88

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	appliance físico deve possuir, pelo menos, 6 (seis) interfaces 1000Base-T e 2 (duas) interfaces 1 Gigabit Ethernet padrão 1GBase-LX para permitir a conexão com a rede; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar os cabos de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 12. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 13. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 768 (setecentos e sessenta e oito) portas de switch ou um total de 24 (vinte e quatro) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 48 (quarenta e oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja,				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 6.5 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPSEc deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSEc deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar Single-Sign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 715 (setecentos e quinze) Mbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116. A solução deverá ser capaz de tratar 1.8 Gbps (HTTP 64K) de tráfego por meio do filtro de aplicações; 117. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120. A solução deverá permitir a criação manual de novos padrões de aplicações; 121. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126. A solução deve permitir a configuração				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129. A solução deverá ser capaz de tratar 10 (dez) Gbps de tráfego por meio das regras de firewall stateful 512 Byte; 130. A solução deverá ser capaz de suportar 1.500.000 (um milhão e quinhentos mil) de sessões simultâneas/concorrentes e 45.000 (quarenta e cinco) novas sessões por segundo; 131. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133. A solução deverá suportar PBR – Policy Based Routing; 134. A solução deverá suportar roteamento multicast; 135. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137. A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 146. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 153. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155. A solução deverá suportar Netflow ou sFlow; 156. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 161. A solução deve possuir ferramentas de diagnósticos e debug 162. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164. A solução deve suportar comunicação com elementos externos através de REST API; 165. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V - atendimento aos princípios: a. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 167. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 168. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
28	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 4 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 16 (dezesesseis) interfaces 1 Gigabit Ethernet padrão 1000Base-T ou 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Caso sejam ofertadas interfaces 10GBase-X, devem ser fornecidos 2 (dois) transceivers 10GBase-SX; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação redundante com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 7. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 8. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 9. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 10. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 11. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 12. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 13. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 14. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 15. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 1.152 (um mil e cento e cinquenta e dois) portas de switch ou um total de 32 (trinta e dois) switches; 16. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 17. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 18. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 19. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 20. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 24. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 25. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 26. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 64 (sessenta e quatro) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 27. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 28. A solução deverá ser capaz de gerenciar	UNIDADE	5	28.226,36	141.131,80

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 29. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 30. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 31. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 32. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 33. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 34. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de listas de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 35. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 36. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 37. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 38. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 39. A solução deverá ser capaz de encaminhar 11.5 Gbps de tráfego encapsulado via VPN IPSec; 40. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 41. A VPN IPSEC deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 42. A VPN IPSEC deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 43. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 44. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 45. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 46. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 47. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 48. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 49. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 50. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 51. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 52. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 53. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como Rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 54. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 55. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 56. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	assim o broadcast e aumentando a disponibilidade de endereços IP; 57. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 58. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 59. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 60. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 61. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 62. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 63. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 64. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 65. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 66. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 67. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 68. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 69. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 70. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 71. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 72. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 73. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 74. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 75. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 76. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 77. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 78. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 79. A solução deve ser capaz de implementar mecanismos de proteção contra-ataques do tipo ARP Poisoning na rede sem fio; 80. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 81. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 82. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 83. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	em um determinado SSID; 84. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 85. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 86. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 87. A solução deverá suportar SingleSign-On (SSO); 88. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 89. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 90. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 91. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informarem as credenciais válidas para acesso à rede; 92. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 93. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 94. A solução deve permitir a configuração do captive portal com endereço IPv6; 95. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 96. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 97. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 98. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 99. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 100. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 101. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 102. A solução deverá ser capaz de inspecionar 1 (Um) Gbps de tráfego SSL; 103. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 104. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 105. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 106. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 107. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 108. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 109. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios pré-configurados em sua base de conhecimento; 110. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 111. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 112. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 113. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 114. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 115. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 116.A solução deverá ser capaz de tratar 2.2 Gbps de tráfego por meio do filtro de aplicações; 117.A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 118.A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 119.A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 120.A solução deverá permitir a criação manual de novos padrões de aplicações; 121.A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 122.A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 123.A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 124.A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 125.A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 126.A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 127.A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 128.A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 129.A solução deverá ser capaz de tratar 18 Gbps de tráfego por meio das regras de firewall stateful 512 byte; 130.A solução deverá ser capaz de suportar 1.500.000 (Um milhão e quinhentos) de sessões simultâneas/concorrentes e 56.000 (cinquenta e seis) novas sessões por segundo; 131.A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 132.A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 133.A solução deverá suportar PBR – Policy Based Routing; 134.A solução deverá suportar roteamento multicast; 135.A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 136.A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 137.A solução deverá possuir suporte a criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 138.A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 139.A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 140.A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 141.A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 142.A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 143.A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 144.A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 145.A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 146.A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 147.A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 148.A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 149.A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 150.A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 151.A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 152.A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	permitir a atualização do firmware desses elementos via interface gráfica; 153.A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 154.A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 155.A solução deverá suportar Netflow ou sFlow; 156.A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 157.Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 158.A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 159.A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 160.A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 161.A solução deve possuir ferramentas de diagnósticos e debug 162.A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 163.Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 164.A solução deve suportar comunicação com elementos externos através de REST API; 165.A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 166.Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 167.Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: a) da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 168.A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 169.A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
29	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 5 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 15 (quinze) interfaces 1 Gigabit Ethernet padrão 1000Base-T e 4 (quatro) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Adicionalmente devem ser fornecidos 2 (dois) transceivers SFP+ conforme padrão 10GBase-SR; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação redundante com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. Deve suportar a instalação de fonte de alimentação redundante; 7. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 8. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 9. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 10. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 11. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 12. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 13. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 14. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 15. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 16. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 3072 (três mil e setenta e dois) portas de switch ou um total de 64 (sessenta e quatro) switches; 17. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 18. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados;	UNIDADE	4	52.162,32	208.649,28

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
19.	A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 20. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 24. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 25. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 26. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 27. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 128 (cento e vinte e oito) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 28. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 29. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 30. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 31. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 32. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 33. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 34. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 35. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 36. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 37. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 38. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface do ponto de acesso; 39. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 40. A solução deverá ser capaz de encaminhar 13 Gbps de tráfego encapsulado via VPN IPSec; 41. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 42. A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 43. A VPN IPSec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 44. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 45. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 46. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 47. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 48. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 49. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 50. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 51. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	interface de gerência; 52. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 53. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 54. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 55. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 56. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 57. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 58. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 59. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 60. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 61. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 62. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 63. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 64. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 65. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 66. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 67. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 68. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 69. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 70. A solução deve possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 71. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 72. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 73. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 74. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 75. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 76. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 77. A				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 78. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 79. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 80. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 81. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 82. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 83. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 84. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 85. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 86. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 87. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 88. A solução deverá suportar SingleSign-On (SSO); 89. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 90. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 91. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 92. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede; 93. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 94. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 95. A solução deve permitir a configuração do captive portal com endereço IPv6; 96. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 97. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 98. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 99. A solução deve implementar recurso para controle de URLs acessadas na rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 100. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 101. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 102. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 103. A solução deverá ser capaz de inspecionar 4 Gbps de tráfego SSL; 104. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 105. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 106. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 107. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 109. A solução deve atualizar periodicamente e				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 110.A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 111.A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 112.A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 113.A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 114.O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 115.A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 116.A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 117.A solução deverá ser capaz de tratar 13 Gbps de tráfego por meio do filtro de aplicações; 118.A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 119.A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 120.A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 121.A solução deverá permitir a criação manual de novos padrões de aplicações; 122.A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 123.A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 124.A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 125.A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 126.A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 127.A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 128.A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 129.A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 130.A solução deverá ser capaz de tratar 27 Gbps de tráfego por meio das regras de firewall stateful 512 byte; 131.A solução deverá ser capaz de suportar 3.000.000 (três milhões) de sessões simultâneas/concorrentes e 280.000 (duzentos e oitenta mil) novas sessões por segundo; 132.A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 133.A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 134.A solução deverá suportar PBR – Policy Based Routing; 135.A solução deverá suportar roteamento multicast; 136.A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 137.A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 138.A solução deverá possuir suporte à criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 139.A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 140.A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 141.A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 142.A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 143.A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 144.A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	ser utilizados como fatores de decisão para encaminhamento do tráfego; 145.A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 146.A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 147.A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 148.A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 149.A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 150.A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 151.A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 152.A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 153.A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 154.A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 155.A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 156.A solução deverá suportar Netflow ou sFlow; 157.A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 158.Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 159.A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 160.A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 161.A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 162.A solução deve possuir ferramentas de diagnósticos e debug 163.A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 164.Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 165.A solução deve suportar comunicação com elementos externos através de REST API; 166.A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 167.Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: 168.da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 169.A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 170.A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				
30	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 6 Características Mínimas: 1. Deve ser fornecida solução para gerenciamento da segurança e infraestrutura da rede capaz de monitorar, administrar e controlar de maneira centralizada os acessos na rede do campus; 2. Deve ser composta por elemento ou elementos fornecidos na forma de appliance físico, ou seja, cada elemento deverá ser composto pelo conjunto de hardware e software do respectivo fabricante; 3. Cada appliance físico deve possuir, pelo menos, 8 (oito) interfaces 1 Gigabit Ethernet padrão 1000Base-T e 2 (duas) interfaces 10 Gigabit Ethernet padrão 10GBase-X para permitir a conexão com a rede. Adicionalmente devem ser fornecidos 2 (dois) transceivers SFP+ conforme padrão 10GBase-SR; 4. Deve possuir interface console com conector RJ-45 ou USB para gerenciamento local; 5. Cada appliance físico deve possuir fonte de alimentação com capacidade de operação em tensões de 100 até 240VAC. Deve acompanhar o cabo de alimentação; 6. Deve suportar a instalação de fonte de alimentação redundante; 7. A solução deverá suportar alta disponibilidade por meio da adição futura de elemento redundante capaz de assumir as funções do elemento principal em caso de falhas; 8. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos; 9. A solução deve conter elemento capaz de realizar o gerenciamento unificado dos pontos de acesso e switches deste processo; 10. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de	UNIDADE	2	180.481,52	360.963,04

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 11. Permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 12. A solução deve permitir a configuração e administração dos switches e pontos de acesso por meio de interface gráfica; 13. A solução deve realizar o gerenciamento de inventário de hardware, software e configuração dos switches e pontos de acesso; 14. A solução deve apresentar graficamente a topologia lógica da rede, representar o status dos elementos por ela gerenciados, além de informações sobre os usuários conectados com a quantidade de dados transmitidos e recebidos por eles; 15. A solução deve monitorar a rede e apresentar indicadores de saúde dos switches e pontos de acesso por ela gerenciados; 16. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 4608 (quatro mil e seiscentos e oito) portas de switch ou um total de 96 (noventa e seis) switches; 17. A solução deve apresentar topologia representando a conexão física dos switches por ela gerenciados, ilustrando graficamente status dos uplinks para identificação de eventuais problemas; 18. A solução deve permitir, através da interface gráfica, configurar VLANs e distribuí-las automaticamente nos switches e pontos de acesso por ela gerenciados; 19. A solução deve, através da interface gráfica, ser capaz de aplicar a VLAN nativa (untagged) e as VLANs permitidas (tagged) nas interfaces dos switches; 20. A solução deve ser capaz de aplicar as políticas de QoS nas interfaces dos switches; 21. A solução deve, através da interface gráfica, ser capaz de aplicar as políticas de segurança para autenticação 802.1X nas interfaces dos switches; 22. A solução deve, através da interface gráfica, ser capaz de habilitar ou desabilitar o PoE nas interfaces dos switches; 23. A solução deve, através da interface gráfica, ser capaz de aplicar ferramentas de segurança, tal como DHCP Snooping, nas interfaces dos switches; 24. A solução deve, através da interface gráfica, ser capaz de realizar configurações do protocolo Spanning Tree nas interfaces dos switches, tal como habilitar ou desabilitar os seguintes recursos: Loop Guard, Root Guard e BPDU Guard; 25. A solução deve monitorar o consumo PoE das interfaces nos switches e apresentar esta informação de maneira gráfica; 26. A solução deve apresentar graficamente informações sobre erros nas interfaces dos switches; 27. A solução deve estar pronta e licenciada para garantir o gerenciamento centralizado de 512 (quinhentos e doze) pontos de acesso wireless simultaneamente. As licenças devem ser válidas para o gerenciamento dos pontos de acesso sem restrições, inclusive sem diferenciar se os pontos de acesso a serem gerenciados serão do tipo indoor ou outdoor; 28. A solução deve permitir a conexão de dispositivos wireless que implementem os padrões IEEE 802.11a/b/g/n/ac/ax; 29. A solução deverá ser capaz de gerenciar pontos de acesso do tipo indoor e outdoor que estejam conectados na mesma rede ou remotamente através de links WAN e Internet; 30. A solução deve permitir a adição de planta baixa do pavimento para ilustrar graficamente a localização geográfica e status de operação dos pontos de acesso por ela gerenciados. Deve permitir a adição de plantas baixas nos seguintes formatos: JPEG, PNG, GIF ou CAD; 31. A solução deve permitir a conexão de dispositivos que transmitam tráfego IPv4 e IPv6; 32. A solução deve otimizar o desempenho e a cobertura wireless (RF) nos pontos de acesso por ela gerenciados, realizando automaticamente o ajuste de potência e a distribuição adequada de canais a serem utilizados. A solução deve permitir ainda desabilitar o ajuste automático de potência e canais quando necessário; 33. A solução deve permitir agendar dia e horário em que ocorrerá a otimização do provisionamento automático de canais nos Access Points; 34. A solução deve suportar a configuração de SSIDs em modo túnel, de tal forma que haverá um elemento com função de concentrador VPN para estabelecimento de túnel com os pontos de acesso por ela gerenciados, estes que deverão ser capazes de encaminhar o tráfego dos dispositivos conectados ao SSID através do túnel; 35. A solução deve permitir habilitar o recurso de Split-Tunneling em cada SSID. Com este recurso, o AP deve suportar a criação de lista de exceções com endereços de serviços da rede local que não devem ter os pacotes enviados pelo túnel até o concentrador, ou seja, todos os pacotes serão encapsulados via VPN, exceto aqueles que tenham como destino os endereços especificados nas listas de exceção; 36. Adicionalmente, a solução deve suportar a configuração de SSIDs com modo de encaminhamento de tráfego conhecido como Bridge Mode ou Local Switching. Neste modo todo o tráfego dos dispositivos conectados em um determinado SSID deve ser comutado localmente na interface ethernet do ponto de acesso e não devem ser encaminhados via túnel; 37. Operando em Bridge Mode ou Local Switch, quando ocorrer falha na comunicação entre o elemento gerenciador e pontos de acesso os clientes devem permanecer conectados ao mesmo SSID para garantir a continuidade na transferência de dados, além de permitir que novos clientes sejam admitidos à rede, mesmo quando o SSID estiver configurado com autenticação 802.1X; 38. A solução deve permitir definir quais redes terão tráfego encaminhado via túnel até o elemento concentrador e quais redes serão comutadas diretamente pela interface				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	do ponto de acesso; 39. A solução deverá ainda, ser capaz de estabelecer túneis VPN dos tipos IPSec e SSL com elementos externos; 40. A solução deverá ser capaz de encaminhar 20 Gbps de tráfego encapsulado via VPN IPSec; 41. A solução deverá suportar os algoritmos de criptografia para túneis VPN: AES, DES, 3DES; 42. A VPN IPSec deverá suportar AES 128, 192 e 256 (Advanced Encryption Standard); 43. A VPN IPSec deverá suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14; 44. A solução deverá possuir suporte a certificados PKI X.509 para construção de VPNs; 45. A solução deverá permitir a customização da porta lógica utilizada pela VPN IPSec; 46. A solução deverá ser capaz de atuar como um cliente de VPN SSL; 47. A solução deverá possuir capacidade de realizar SSL VPNs utilizando certificados digitais; 48. A solução deverá suportar autenticação de 02 (dois) fatores para a VPN SSL; 49. A Solução deverá ser capaz de prover uma arquitetura de Auto Discovery VPN – ADVPN ou tecnologia similar; 50. A solução deve implementar recursos que possibilitem a identificação de interferências provenientes de equipamentos que operem nas frequências de 2.4GHz e 5GHz; 51. A solução deve implementar recursos de análise de espectro que possibilitem a identificação de interferências provenientes de equipamentos não-WiFi e que operem nas frequências de 2.4GHz ou 5GHz. A solução deve ainda apresentar o resultado dessas análises de maneira gráfica na interface de gerência; 52. A solução deverá detectar Receiver Start of Packet (RX-SOP) em pacotes wireless e ser capaz de ignorar os pacotes que estejam abaixo de determinado limiar especificado em dBm; 53. A solução deve permitir o balanceamento de carga dos usuários conectados à infraestrutura wireless de forma automática. A distribuição dos usuários entre os pontos de acesso próximos deve ocorrer sem intervenção humana e baseada em critérios como número de dispositivos associados em cada ponto de acesso; 54. A solução deve possuir mecanismos para detecção e mitigação de pontos de acesso não autorizados, também conhecidos como rogue APs. A mitigação deverá ocorrer de forma automática e baseada em critérios, tais como: intensidade de sinal ou SSID. Os pontos de acesso gerenciados pela solução devem evitar a conexão de clientes em pontos de acesso não autorizados; 55. A solução deve identificar automaticamente pontos de acesso intrusos que estejam conectados na rede cabeada (LAN). A solução deve ser capaz de identificar o ponto de acesso intruso mesmo quando o MAC Address da interface LAN for ligeiramente diferente (adjacente) do MAC Address da interface WLAN; 56. A solução deve permitir a configuração individual dos rádios do ponto de acesso para que operem no modo monitor/sensor, ou seja, com função dedicada para detectar ameaças na rede sem fio e com isso permitir maior flexibilidade no design da rede wireless; 57. A solução deve permitir o agrupamento de VLANs para que sejam distribuídas múltiplas subredes em um determinado SSID, reduzindo assim o broadcast e aumentando a disponibilidade de endereços IP; 58. A solução deve permitir a criação de múltiplos domínios de mobilidade (SSID) com configurações distintas de segurança e rede. Deve ser possível especificar em quais pontos de acesso ou grupos de pontos de acesso que cada domínio será habilitado; 59. A solução deve permitir ao administrador da rede determinar os horários e dias da semana que as redes (SSIDs) estarão disponíveis aos usuários; 60. A solução deve permitir restringir o número máximo de dispositivos conectados por ponto de acesso e por rádio; 61. A solução deve suportar o padrão IEEE 802.11r para acelerar o processo de roaming dos dispositivos através do recurso conhecido como Fast Roaming; 62. A solução deve suportar o padrão IEEE 802.11k para permitir que um dispositivo conectado à rede wireless identifique rapidamente outros pontos de acesso disponíveis em sua área para que ele execute o roaming; 63. A solução deve suportar o padrão IEEE 802.11v para permitir que a rede influencie as decisões de roaming do cliente conectado através do fornecimento de informações complementares, tal como a carga de utilização dos pontos de acesso que estão próximos; 64. A solução deve suportar o padrão IEEE 802.11w para prevenir ataques à infraestrutura wireless; 65. A solução deve suportar priorização na rede wireless via WMM e permitir a tradução dos valores para DSCP quando os pacotes forem destinados à rede cabeada; 66. A solução deve implementar técnicas de Call Admission Control para limitar o número de chamadas simultâneas na rede sem fio; 67. A solução deve apresentar informações sobre os dispositivos conectados à infraestrutura wireless e informar ao menos as seguintes informações: Nome do usuário conectado ao dispositivo, fabricante e sistema operacional do dispositivo, endereço IP, SSID ao qual está conectado, ponto de acesso ao qual está conectado, canal ao qual está conectado, banda transmitida e recebida (em Kbps), intensidade do sinal considerando o ruído em dB (SNR), capacidade MIMO e horário da associação; 68. Para garantir uma melhor distribuição de dispositivos entre as frequências disponíveis e resultar em melhorias na utilização da radiofrequência, a solução deve ser capaz de distribuir automaticamente os dispositivos dual-band para que conectem primariamente em 5GHz através do recurso conhecido como Band Steering; 69. A solução deve permitir a configuração de quais data rates estarão ativos e quais serão desabilitados; 70. A solução deve				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	possuir recurso capaz de converter pacotes Multicast em pacotes Unicast quando forem encaminhados aos dispositivos que estiverem conectados à infraestrutura wireless, melhorando assim o consumo de Airtime; 71. A solução deve permitir a configuração dos parâmetros BLE (Bluetooth Low Energy) nos pontos de acesso; 72. A solução deve suportar recurso que ignore Probe Requests de clientes que estejam com sinal fraco ou distantes. Deve permitir definir o limiar para que os Probe Requests sejam ignorados; 73. A solução deve suportar recurso para automaticamente desconectar clientes wireless que estejam com sinal fraco ou distantes. Deve permitir definir o limiar de sinal para que os clientes sejam desconectados; 74. A solução deve suportar recurso conhecido como Airtime Fairness (ATF) para controlar o uso de airtime nos SSIDs; 75. A solução deve ser capaz de reconfigurar automaticamente e de maneira autônoma os pontos de acesso para que desativem a conexão de clientes nos rádios 2.4GHz quando for identificado um alto índice de sobreposição de sinal oriundo de outros pontos de acesso gerenciados pela mesma infraestrutura, evitando assim interferências; 76. A solução deve permitir que os usuários da rede sem fio sejam capazes de acessar serviços disponibilizados através do protocolo Bonjour (L2) e que estejam hospedados em outras subredes, tais como: AirPlay e Chromecast. Deve ser possível especificar em quais VLANs o serviço será disponibilizado; 77. A solução deve permitir a configuração de redes Mesh entre os pontos de acesso por ela gerenciados. Deve permitir ainda que sejam estabelecidas conexões mesh entre pontos de acesso do tipo indoor com pontos de acesso do tipo outdoor; 78. A solução deve implementar mecanismos de proteção para identificar ataques à infraestrutura wireless. Ao menos os seguintes ataques devem ser identificados: a. Ataques de flood contra o protocolo EAPOL (EAPOL Flooding); b. Os seguintes ataques de negação de serviço: Association Flood, Authentication Flood, Broadcast Deauthentication e Spoofed Deauthentication; c. ASLEAP; d. Null Probe Response or Null SSID Probe Response; e. Long Duration; f. Ataques contra Wireless Bridges; g. Weak WEP; h. Invalid MAC OUI. 79. A solução deve implementar mecanismos de proteção para mitigar ataques à infraestrutura wireless. Ao menos ataques de negação de serviço devem ser mitigados pela infraestrutura através do envio de pacotes de deauthentication; 80. A solução deve ser capaz de implementar mecanismos de proteção contra ataques do tipo ARP Poisoning na rede sem fio; 81. Permitir configurar o bloqueio de comunicação lateral entre os clientes wireless conectados a um determinado SSID; 82. Em conjunto com os pontos de acesso, a solução deve implementar os seguintes métodos de autenticação: WPA (TKIP) e WPA2 (AES); 83. Em conjunto com os pontos de acesso, a solução deve ser compatível e implementar o método de autenticação WPA3; 84. A solução deve permitir a configuração de múltiplas chaves de autenticação PSK para utilização em um determinado SSID; 85. Quando usando o recurso de múltiplas chaves PSK, a solução deve permitir a definição de limite quanto ao número de conexões simultâneas para cada chave criada; 86. Em conjunto com os pontos de acesso, a solução deve suportar os seguintes métodos de autenticação EAP: EAP-TLS, EAP-TTLS e PEAP; 87. A solução deverá possuir integração com servidores RADIUS, LDAP e Microsoft Active Directory para autenticação de usuários; 88. A solução deverá suportar SingleSign-On (SSO); 89. A solução deve implementar recurso de controle de acesso à rede (NAC - Network Access Control), identificando automaticamente o tipo de equipamento conectado (profiling) e atribuindo de maneira automática a política de acesso à rede. Este recurso deve estar disponível para conexões na rede sem fio e rede cabeada; 90. A solução deve implementar o protocolo IEEE 802.1X com associação dinâmica de VLANs para os usuários das redes sem fio e cabeada, com base nos atributos fornecidos pelos servidores RADIUS; 91. A solução deve implementar o mecanismo de mudança de autorização dinâmica para 802.1X, conhecido como RADIUS CoA (Change of Authorization) para autenticações nas redes sem fio e cabeada; 92. A solução deve implementar recurso para autenticação de usuários conectados às redes sem fio e cabeada através de página web HTTPS, também conhecido como Captive Portal. A solução deve limitar o acesso dos usuários enquanto estes não informar as credenciais válidas para acesso à rede; 93. A solução deve permitir a customização da página de autenticação do captive portal, de forma que o administrador de rede seja capaz de alterar o código HTML da página web formatando texto e inserindo imagens; 94. A solução deve permitir a coleta de endereço de e-mail dos usuários como método de autorização para ingresso à rede; 95. A solução deve permitir a configuração do captive portal com endereço IPv6; 96. A solução deve permitir o cadastramento de contas para usuários visitantes localmente. A solução deve permitir ainda que seja definido um prazo de validade para a conta criada; 97. A solução deve possuir interface gráfica para administração e gerenciamento exclusivo das contas de usuários visitantes, não permitindo acesso às demais funções de administração da solução; 98. Após a criação de um usuário visitante, a solução deve enviar as credenciais por e-mail para o usuário cadastrado; 99. A solução deve implementar recurso para controle de URLs acessadas na				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	rede através de análise dos protocolos HTTP e HTTPS. Deve possuir uma base de conhecimento para categorização das URLs e permitir configurar quais categorias serão permitidas e bloqueadas de acordo com o perfil dos usuários; 100. A solução deverá permitir especificar um determinado horário ou período (dia, mês, ano, dia da semana e hora) para que uma política de controle de URL seja imposta aos usuários; 101. A solução deverá permitir a operação tanto em modo proxy explícito quanto em modo proxy transparente; 102. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos websites acessados na rede; 103. A solução deverá ser capaz de inspecionar 8 Gbps de tráfego SSL; 104. O administrador da rede deve ser capaz de adicionar manualmente URLs e expressões regulares que deverão ser bloqueadas ou permitidas independente da sua categoria; 105. A solução deverá permitir a customização de página de bloqueio apresentada aos usuários; 106. Ao bloquear o acesso de um usuário a um determinado website, a solução deve permitir notificá-lo da restrição e ao mesmo tempo dar-lhe a opção de continuar sua navegação ao mesmo site através de um botão do tipo continuar; 107. A solução deverá possuir uma blacklist contendo URLs de certificados maliciosos em sua base de dados; 108. A solução deve registrar todos os logs de eventos com bloqueios e liberações das URLs acessadas; 109. A solução deve atualizar periodicamente e automaticamente a base de URLs durante toda a vigência do prazo de garantia da solução; 110. A solução deve implementar solução de segurança baseada em filtragem do protocolo DNS com múltiplas categorias de websites/domínios préconfigurados em sua base de conhecimento; 111. A ferramenta de filtragem do protocolo DNS deve garantir que o administrador da rede seja capaz de criar políticas de segurança para liberar, bloquear ou monitorar o acesso aos websites/domínios para cada categoria e também para websites/domínios específicos; 112. A solução deve registrar todos os logs de eventos com bloqueios e liberações dos acessos aos websites/domínios que passaram pelo filtro de DNS; 113. A ferramenta de filtragem do protocolo DNS deve identificar os domínios utilizados por Botnets para ataques do tipo Command & Control (C&C) e bloquear acessos e consultas oriundas da rede com destino a estes domínios maliciosos. Os usuários não deverão ser capazes de resolver os endereços dos domínios maliciosos através de consultas do tipo nslookup e/ou dig; 114. O recurso de filtragem do protocolo DNS deve ser capaz de filtrar consultas DNS em IPv6; 115. A solução deve possuir capacidade de reconhecimento de aplicações através da técnica de DPI (Deep Packet Inspection) que permita ao administrador da rede monitorar o perfil de acesso dos usuários e implementar políticas de controle para tráfego IPv4 e IPv6. Deve permitir o funcionamento deste recurso durante todo o período de garantia da solução; 116. A solução deve ser capaz de inspecionar o tráfego encriptado em SSL para uma análise mais profunda dos pacotes, a fim de possibilitar a identificação de aplicações conhecidas; 117. A solução deverá ser capaz de tratar 15 Gbps de tráfego por meio do filtro de aplicações; 118. A solução deve registrar todos os logs de eventos com bloqueios e liberações das aplicações que foram acessadas na rede; 119. A base de reconhecimento de aplicações através de DPI deve identificar, no mínimo, 2000 (duas mil) aplicações; 120. A solução deve atualizar periodicamente e automaticamente a base de aplicações durante toda a vigência do prazo de garantia da solução; 121. A solução deverá permitir a criação manual de novos padrões de aplicações; 122. A solução deve permitir a criação de regras para bloqueio e limite de banda (em Mbps, Kbps ou Bps) para as aplicações reconhecidas através da técnica de DPI; 123. A solução deve permitir aplicar regras de bloqueio e limites de banda para, no mínimo, 10 aplicações de maneira simultânea em cada regra; 124. A solução deve ainda, através da técnica de DPI, reconhecer aplicações sensíveis ao negócio e permitir a priorização deste tráfego com marcação QoS; 125. A solução deve monitorar e classificar o risco das aplicações acessadas pelos clientes na rede; 126. A solução deve ser capaz de implementar regras de firewall stateful para controle do tráfego permitindo ou descartando pacotes de acordo com a política configurada, regras estas que devem usar como critérios dia e hora, endereços de origem e destino (IPv4 e IPv6), portas e protocolos; 127. A solução deve permitir a configuração de regras de identity-based firewall, ou seja, deve permitir que grupos de usuários sejam utilizados como critério para permitir ou bloquear o tráfego; 128. A solução deverá ter a capacidade de criar políticas de firewall baseando-se em endereços MAC; 129. A solução deverá permitir a utilização de endereços FQDN nas políticas de firewall; 130. A solução deverá ser capaz de tratar 36 Gbps de tráfego por meio das regras de firewall stateful 512 byte; 131. A solução deverá ser capaz de suportar 8.000.000 (oito milhões) de sessões simultâneas/concorrentes e 450.000 (quatrocentos e cinquenta mil) novas sessões por segundo; 132. A solução deverá possuir a funcionalidade de tradução de endereços estáticos – NAT (Network Address Translation) dos seguintes tipos: um para um, N-para-um, vários para um, NAT64, NAT66, NAT46 e PAT; 133. A solução deve suportar os protocolos OSPF e BGP em IPv4 e IPv6 para compartilhamento de rotas dinâmicas entre a infraestrutura; 134. A				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	solução deverá suportar PBR – Policy Based Routing; 135. A solução deverá suportar roteamento multicast; 136. A solução deverá possuir mecanismo de anti-spoofing tipo RPF (Reverse Path Forward) ou similar; 137. A solução deverá possuir mecanismo de tratamento para aplicações multimídia (session-helpers ou ALGs) tipo SIP e H323; 138. A solução deverá possuir suporte à criação de, no mínimo, 10 (dez) sistemas virtuais internos ao(s) elemento(s) de filtragem de tráfego que garantam a segregação e possam ser administrados por equipes distintas; 139. A solução deverá permitir limitar o uso de recursos utilizados por cada sistema virtual interno ao(s) elemento(s) de filtragem de tráfego; 140. A solução deverá possuir conectores SDN capazes de sincronizar objetos automaticamente com elementos externos, inclusive provedores de nuvem pública; 141. A solução deverá ser capaz de utilizar a tecnologia de SD-WAN para distribuir automaticamente o tráfego de múltiplos links por meio de uma interface virtual agregada; 142. A solução deverá ser capaz de indicar como rota padrão de todo o tráfego a interface virtual agregada; 143. A solução deverá permitir a adição de, no mínimo, 04 (quatro) interfaces de dados, sejam elas links de operadoras e/ou túneis VPN IPSec, para que componham a interface virtual agregada; 144. A solução deverá ser capaz de mensurar a saúde do link baseando-se em critérios mínimos de: Latência, Jitter e Packet Loss. Deve ser possível configurar um valor de Threshold para cada um destes critérios, estes que poderão ser utilizados como fatores de decisão para encaminhamento do tráfego; 145. A solução deverá permitir a criação de política de traffic shaping que defina em valores percentuais uma parte da largura de banda que deverá ser reservada para uma aplicação do total de largura de banda disponível na interface virtual agregada; 146. A solução deverá implementar método de correção de erros de pacotes em túneis de VPN IPSec; 147. A solução deverá permitir a realização de testes dos links via probes que utilizem os seguintes métodos: Ping, HTTP, TCP-Echo e UDP-Echo. 148. A solução deverá permitir marcar com DSCP os pacotes utilizando durante os testes de link (probes) para obter uma avaliação mais realista da qualidade de um determinado link; 149. A solução deverá possibilitar a distribuição de peso em cada um dos links que compõe a interface virtual agregada, a critério do administrador, de forma que o algoritmo de balanceamento utilizado possa ser baseado em: número de sessões, volume de tráfego, IP de origem e destino e/ou transbordo de link (Spillover). 150. A solução deve ser capaz de implementar função de DHCP Server para IPv4 e IPv6; 151. A solução deve ser capaz de configurar parâmetros SNMP nos switches e pontos de acesso; 152. A solução deve possuir recurso para realizar testes de conectividade nos pontos de acesso a fim de validar se as VLAN estão apropriadamente configuradas no switch ao qual os APs estejam fisicamente conectados; 153. A solução deve identificar o firmware utilizado em cada ponto de acesso e switch por ela gerenciado, além de permitir a atualização do firmware desses elementos via interface gráfica; 154. A solução deve permitir a atualização de firmware individualmente nos pontos de acesso e switches, garantindo a gestão e operação simultânea com imagem de firmwares diferentes; 155. A solução deve recomendar versões de firmware a ser instalado nos switches e pontos de acesso por ela gerenciados; 156. A solução deverá suportar Netflow ou sFlow; 157. A solução deverá ser gerenciada através dos protocolos HTTPS e SSH em IPv4 e IPv6; 158. Deve implementar autenticação administrativa através do protocolo RADIUS ou TACACS; 159. A solução deve permitir o envio dos logs para múltiplos servidores syslog externos; 160. A solução deve permitir ser gerenciada através do protocolo SNMP, além de emitir notificações através da geração de traps; 161. A solução deve permitir a captura de pacotes e exportá-los em arquivos com formato .pcap; 162. A solução deve possuir ferramentas de diagnósticos e debug 163. A solução deve enviar e-mail de notificação aos administradores da rede em caso de evento de indisponibilidade de algum elemento por ela gerenciado ou em caso de evento de falha; 164. Deve registrar eventos para auditoria dos acessos e mudanças de configuração realizadas por usuários; 165. A solução deve suportar comunicação com elementos externos através de REST API; 166. A solução deverá ser compatível e gerenciar os pontos de acesso e switches deste processo; 167. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 envio de peças/equipamentos de reposição em até 3 dias úteis; 164. Conforme disposto no inciso V, alínea a, do artigo 40 da lei 14.133, de 01 de abril de 2021 (V – atendimento aos princípios: 168. da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho;) este equipamento, por questões de compatibilidade, gerência, suporte e garantia, deve ser do mesmo fabricante dos demais equipamentos deste grupo (lote). 169. A CONTRATADA deve garantir ao CONTRATANTE o pleno acesso ao site do fabricante do produto, com direito a consultar quaisquer bases de dados disponíveis para usuários e a efetuar downloads das atualizações do software, atualização de listas e informações ou documentação do software que compõem a solução. 170. A CONTRATANTE será responsável pela abertura de chamado junto ao fabricante, para os problemas relacionados aos produtos ofertados, onde os prazos serão condicionados ao mesmo.				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
37	TREINAMENTO – SOLUÇÃO DE SEGURANÇA DE DADOS Requisitos para a realização de um treinamento em segurança da informação no modelo de repasse de conhecimentos, com foco em Switches, Access Points e Firewall. O objetivo é capacitar uma turma de 23 pessoas, garantindo o conhecimento necessário para utilizar e configurar adequadamente esses dispositivos de rede, com uma carga horária de 8 horas. O treinamento não se refere a linha de treinamentos oficiais dos fabricantes da solução fornecida. ----- 1. Objetivos do Treinamento O treinamento tem como objetivo principal capacitar os participantes nas seguintes áreas: a) Compreensão dos conceitos fundamentais de segurança da informação; b) Familiarização com o funcionamento e as características dos Switches, Access Points e Firewall; c) Conhecimento das melhores práticas para configuração e uso desses dispositivos; d) Identificação e resolução de problemas comuns relacionados à segurança da informação em redes; e) Desenvolvimento de habilidades práticas para lidar com ameaças e incidentes de segurança. 2. Conteúdo Programático O treinamento abordará os seguintes tópicos: a) Princípios de segurança em redes. b) Switches: Funcionamento e características dos Switches; VLANs (Virtual Local Area Networks) e sua importância para a segurança; Implementação de políticas de segurança em Switches. c) Access Points: Funcionamento e características dos Access Points; Configuração de segurança em redes sem fio; Identificação e prevenção de ataques em redes sem fio. d) Firewall: Funcionamento e características de um Firewall; Configuração de regras de segurança em Firewalls; Detecção e resposta a incidentes de segurança utilizando Firewalls. e) Práticas recomendadas e estudos de caso: Melhores práticas para segurança da informação em redes; Estudos de caso para análise e resolução de problemas relacionados à segurança. Metodologia O treinamento será ministrado por profissionais especializados em segurança da informação, utilizando uma abordagem teórica e prática. Serão utilizados recursos audiovisuais, exemplos concretos e exercícios práticos para melhorar a compreensão dos participantes. 3. Carga Horária e Duração O treinamento terá uma carga horária de 8 horas realizado em turma única e em dia único. 4. Público-Alvo O treinamento destina-se aos profissionais da contratante que serão responsáveis pela administração dos equipamentos objeto deste termo. 5. Recursos Necessários O treinamento será realizado remotamente devendo contemplar todos exercícios práticos abordando todas as soluções (Switches, Access Points e Firewall). É responsabilidade do contratante fornecer conexão à Internet e computadores para exercícios práticos e os recursos necessários para a realização do treinamento. 6. Certificados Ao final do treinamento, os participantes receberão certificados de conclusão, atestando sua participação. 7. Cronograma O cronograma do treinamento será definido em conjunto com o contratante, levando em consideração a disponibilidade da turma e a carga horária mínima estabelecida 8. Responsabilidades do Contratante O contratante será responsável por: a) Fornecer os recursos necessários para a realização do treinamento; b) Garantir a participação mínima de 23 pessoas; c) Colaborar na definição do cronograma do treinamento.	SERVIÇO	1	7.278,28	7.278,28
Valor Total do Lote/Grupo: R\$ 2.729.879,58					
LOTE/GRUPO 4: BACKUP DE DADOS					
2	APPLIANCE DE BACKUP - TIPO 1 CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. O hardware do módulo de armazenamento de backup em disco não poderá ser compartilhado com nenhum outro software para operar; 2. Todos os valores de performance e capacidade das especificações desse item devem considerar o sistema de cálculo BASE 10, onde 1TB = 1000GB; 3. Deve possuir recursos de tolerância a falhas de, pelo menos, discos, fontes de alimentação e ventiladores; 4. Possuir baterias, supercapacitores ou tecnologia similar, para proteger a cache de escrita, evitando a perda de dados em eventos de falha elétrica; 5. Deverá permitir a implementação de topologias de replicação, como 1 para 1, 1 para N, N para 1 e o cascadeamento de equipamentos. 6. A solução deve permitir a replicação dos dados retidos para a nuvem pública; 7. Deve ser fornecida com discos rígidos hot-pluggable e hot-swappable, permitindo substituição sem necessidade interrupção do funcionamento da solução; 8. Deve ser entregue com arranjos de discos rígidos do tipo RAID-6 ou RAID-DP, configurado de tal modo a tolerar a falha de até 2 (dois) discos rígidos e contar com ao menos 1 disco de hot-spare para cada RAID group, para os discos destinados ao armazenamento de dados de backup; 9. Deve permitir montagem em rack padrão 19" do CLIENTE e deve ser entregue com todos os trilhos, cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação; 10. Deve possuir, no mínimo, 50 TB (cinquenta terabytes) úteis sem considerar taxa de deduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento; 11. Deve suportar a expansão de sua capacidade para, no mínimo, 450TB (quatrocentos e cinquenta terabytes) de capacidade líquida (sem considerar taxas de deduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento). Esta ampliação de capacidade deverá ser realizada	UNIDADE	2	630.484,09	1.260.968,18

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	através de unidades de expansão, para o mesmo conjunto de armazenamento, mantendo a característica de deduplicação global da solução; 12. Deve possuir pelo menos 2 (duas) interfaces de rede 10 GbE (dez Gigabit Ethernet) para conexão com switch LAN (interconnect) por meio de conector óptico (SFP+) para Backups executados via LAN. Os conectores devem ser fornecidos em conjunto com o equipamento, bem como 2 (dois) cabos DAC de 3 metros compatível com o switch existente. 13. Deve possuir pelo menos 2 (duas) interfaces de rede 1 GbE (um Gigabit Ethernet) para conexão com switch LAN (interconnect) por meio de conector UTP CAT6 para gerenciamento. Os conectores devem ser fornecidos em conjunto com o equipamento; 14. Deve possuir pelo menos 1 (um) Porta IPMI/iLO/iDRAC ou similar; 15 .Deve possuir taxa de transferência de, no mínimo, 5 TB/hora (cinco terabytes por hora) para operações de backup desconsiderando qualquer ganho com compressão e deduplicação na origem (cliente e servidor de backup). 16. Deve ser novo, de primeiro uso, da linha de equipamentos (modelos) mais recentemente anunciada pelo fabricante, estar em linha de fabricação e não ter previsão de EOSL (end of Service life) anunciada para os próximos 5 anos na data da abertura da licitação; 17. Deve constar no site do fabricante (documento oficial e público) como um appliance ou sistema de armazenamento de backup em disco, em linha de produção; 18. Não serão aceitas soluções montadas especificamente para esse certame, composições de soluções em regime de OEM, nem equipamentos usados, remanufaturados, de demonstração ou gateways. ----- SOFTWARE CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. Deve ser homologado e plenamente compatível com o software de proteção existente do fabricante Veeam (utilizado pelo IFSC). 2. Deve corresponder a um sistema inteligente de armazenamento de backup em disco (INDICAR O NÚMERO DO ITEM), que se entende como um subsistema com o propósito específico de armazenamento de backup com compactação, deduplicação e replicação dos dados deduplicados; 3. Não serão aceitas soluções definidas por Software (Virtual Appliance); 4. Deve permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais, já licenciados para a capacidade máxima ofertada no certame; 5. Todas as licenças de software necessárias para o completo atendimento das especificações técnicas dos equipamentos deverão ser ofertadas na modalidade de uso perpétuo, ou seja, os equipamentos deverão continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado, e deverão ser fornecidas na capacidade máxima suportada pelos equipamentos. 6. O sistema ofertado deverá possuir uma arquitetura do tipo "scale-up" ou do tipo "scale-out" assegurando escalabilidade vertical ou horizontal. Consequentemente, não serão aceitas ofertas de sistemas baseados em federação ou cluster de equipamentos de menor porte, se o conjunto do repositório de armazenamento não for capaz de efetuar deduplicação global dos dados retidos entre os dispositivos. Gateways ou composições desenvolvidas e fabricadas exclusivamente para fins de atendimento do objeto do edital não serão aceitas em hipótese alguma. 7. O sistema de armazenamento fornecido deve permitir a adição futura de ao menos mais uma controladora (nó de processamento) no mesmo conjunto de armazenamento para atuar em modo de alta-disponibilidade ativo-passivo (failover) ou ativo-ativo (loadbalance) para as tarefas de backup, de forma que na eventualidade da falha de uma das controladoras (nó de processamento), as atividades de backup possam ser automaticamente redirecionadas para a outra controladora; 8. Deve ser agnóstico ao software de backup, sendo, no mínimo, compatível com os softwares Veritas Netbackup, IBM Spectrum Protect (TSM), Veeam Backup & Recovery, DELL EMC NetWorker e Commvault, garantindo total integração; Possuir mecanismos que protejam contra a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental; 9. Deverá implementar mecanismos de validação da consistência dos dados deduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações. A tecnologia deverá reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas. O mecanismo deve ser nativo do equipamento, não sendo aceitos scripts para atendimento deste item; 10. Deve possuir funcionalidade de deduplicação dos dados em nível de bloco ou bytes, com capacidade de eliminação de dados redundantes para racionalizar a utilização do espaço de armazenamento. Serão aceitas soluções que efetuem a deduplicação em linha (inline) ou em paralelo. Caso possua deduplicação em linha (inline), deve fornecer todo o licenciamento e componentes para ativar essa funcionalidade em toda a volumetria útil entregue. Não serão aceitas soluções que efetuem deduplicação post-processing, requerendo janela de deduplicação, nem limitando a execução de backups, restores e replicações durante a execução do processo de deduplicação; 11. Deve suportar que a deduplicação seja realizada juntamente com as operações de backup e restauração, tornando desnecessária uma janela dedicada para sua execução; 12. Deve possuir deduplicação global, mesmo que o armazenamento				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	esteja dividido em volumes lógicos, sendo capaz de identificar dados duplicados de backups de diferentes origens dentro de um mesmo sistema de modo a maximizar a taxa de deduplicação e garantindo que os dados retidos sejam gravados uma única vez; 13. Deve suportar simultaneamente acessos de leitura e gravação pelos protocolos CIFS, NFS e OST; 14. Deve permitir a execução de processos de backup e restore em paralelo; 15. Deve possuir interface WEB para gerenciamento do sistema de armazenamento de backup; 16. Deve possuir integração com o Microsoft Active Directory 2012 e superiores, para autenticação e definição de perfis de acesso. 17. Deve ainda permitir a configuração de duplo fator de autenticação para acesso ao gerenciamento do sistema via integração com sistemas de senha descartável (senha de uso único, em inglês: One-time password - OTP), tais como Google Authenticator, Microsoft Authenticator ou similares. Caso o equipamento requeira um dispositivo/sistema OTP específico e este necessite de licenciamento, hardwares e/ou infraestrutura próprios (ex. Common Access Card (CAC)/Personal Information Verification (PIV) cards, etc.), o mesmo deve ser fornecido em conjunto (hardwares, softwares, licenças, serviços, etc.) para, no mínimo, 5 usuários; 18. Deve possuir funcionalidade para replicação de backups em site remoto de forma assíncrona entre subsistemas semelhantes do mesmo fabricante, utilizando recursos de deduplicação, permitindo reduzir o consumo do link de comunicação. Essa funcionalidade deve ser suportada pelo mesmo fabricante do subsistema e deve ser entregue licenciada para toda a capacidade fornecida; 19. Deve permitir replicar os dados através de rede IP (WAN/LAN); Deve estar licenciado para replicar todo o sistema de armazenamento de backup, incluindo a capacidade de expansão; 20. Deve permitir que as aplicações Oracle (RMAN) e Microsoft SQL realizem backups do tipo Stream Based (Oracle Stream Backup) e "database dump" diretamente para o equipamento, via CIFS e NFS, sem utilizar o software de backup para evitar, assim, o consumo de suas licenças e sem a necessidade de licenciar os volumes (TBs) ou os servidores de banco de dados (CPU, Tier, Core) junto ao software de backup. Se houver necessidade de licenciar essa funcionalidade no equipamento ofertado, todas as licenças necessárias devem ser inclusas; 21. Deve possuir recursos avançados de cibersegurança para prevenção de ataques cibernéticos do tipo Ransomware garantindo a proteção dos dados retidos, com as seguintes características: 21.1. Tal proteção deve ser do dispositivo de armazenamento ofertado e deverá funcionar de maneira automática e transparente, isto é, independentemente do software/utilitário de backup, sem depender do desenvolvimento de scripts de integração e sem requerer ações ou atividades manuais sobre o dado retido; 21.2. Deve garantir a inviolabilidade (imutabilidade) dos dados retidos, garantindo assim que os dados protegidos não possam ser alterados ou apagados, mesmo se o software de backup ou ambiente operacional onde ele opera ficar sob controle do atacante (hacker, malware). Tal proteção deve garantir que, mesmo nas situações em que o atacante procure expirar o conteúdo dos backups através do catálogo do software de backup, os dados retidos ainda possam ser recuperados por um período de dias; 21.3. Não pode requerer e nem ser recomendada janela específica para a aplicação do recurso de proteção dos dados retidos, considerando o conjunto do Software de Backup envolvido e Equipamento ofertado, ou seja, a proteção deverá ser aplicada de forma imediata, assim que os dados retidos sejam deduplicados; 21.4. Deve fazer uso do conceito de isolamento para a proteção dos dados, ou seja, os dados protegidos deverão estar invisíveis da superfície de ataque, isto é, não poderão ser acessados através da rede nem pelo software/utilitário de backup. 21.5. Possuir recurso de dupla autorização (Dual Authorization - Dual Auth), ou seja, alterações das configurações contra Ransomware deverão ser aprovadas por um segundo usuário; 22. Deve possuir recursos para monitoramento remoto pelo fabricante, tal como notificação do tipo Call-Home, para verificação proativa de componentes de hardware em situação de falha ou pré-falha; 23. Deve possuir suporte aos protocolos de monitoramento SNMP e Syslog; ----- SUPORTE E GARANTIA CARACTERÍSTICAS MÍNIMAS OBRIGATORIAS: 1. A CONTRATADA deverá fornecer juntamente com a solução de armazenamento de backup acesso a um engenheiro de suporte nomeado de 2º nível do fabricante (nível onde o analista de suporte é qualificado para atuar diretamente no problema, sem necessidade de triagem prévia), que atuará como ponto único de contato para fornecer assistência avançada de forma remota em horário comercial. Caso este engenheiro de suporte esteja temporariamente indisponível, deve ser dado a opção de o caso ser redirecionado para um outro engenheiro de suporte também de 2º nível. O engenheiro de suporte do fabricante deve, adicionalmente, realizar durante todo o período de garantia as seguintes atividades: atualização da solução de armazenamento de backup, verificações proativas junto ao CONTRATANTE, esclarecimento de dúvidas técnicas e apoio em atividades de revisão e alteração de configurações do dia a dia. 2. Caso a CONTRATADA não consiga atender ao nível de suporte exigido com recurso nomeado de 2º nível, será aceito o fornecimento de serviços na modalidade remoto como				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	forma de atendimento, desde que seja do próprio fabricante e seja disponibilizado recurso humano certificado tecnicamente na solução no qual será ponto único de contato para todas as questões relacionadas a suporte técnico, incluindo abertura e acompanhamento de ponta-a-ponta dos casos de suporte, assim como das demais atividades listadas. 3. Durante a vigência da garantia, deverão ser instaladas, sem custos adicionais, todas as atualizações, alterações e melhorias introduzidas nos softwares objetos da presente contratação imediatamente a sua homologação e publicação, buscando assim garantir que a solução esteja nas conformidades recomendadas pelo fabricante, desde que compatíveis com o equipamento adquirido; 4. O atendimento de suporte remoto do fabricante deve permitir, sem limite de quantidade, durante a vigência da garantia, que o suporte remoto realize, pelo menos, as seguintes tarefas: instalação de correções e atualizações, revisão das configurações e sugestão de melhores práticas do fabricante, reconfiguração e reinstalação do appliance, quando for necessário; 5. Deve ser ofertado garantia e suporte técnico para a solução por um período mínimo de 3 anos. ----- ----- SERVIÇO DE INSTALAÇÃO (HARDWARE, SOFTWARE E GARANTIA) CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. Deverá ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados. 2. O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte: 2.1. Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados; 2.2. Conexão e configuração do appliance de backup no switch de rede do Contratante; 2.3. Atualização de softwares, firmwares e drives que compõem a solução; 2.4. Instalação, configuração e aplicação das licenças aplicáveis; 2.5. Documentação do ambiente configurado e instalado. 2.6. A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o appliance de backup em condições de pleno funcionamento.				
3	APPLIANCE DE BACKUP - TIPO 2 CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. O hardware do módulo de armazenamento de backup em disco não poderá ser compartilhado com nenhum outro software para operar; 2. Todos os valores de performance e capacidade das especificações desse item devem considerar o sistema de cálculo BASE 10, onde 1TB = 1000GB; 3. Deve possuir recursos de tolerância a falhas de, pelo menos, discos, fontes de alimentação e ventiladores; 4. Possuir baterias, supercapacitores ou tecnologia similar, para proteger a cache de escrita, evitando a perda de dados em eventos de falha elétrica; 5. Deverá permitir a implementação de topologias de replicação, como 1 para 1, 1 para N, N para 1 e o cascadeamento de equipamentos. A solução deve permitir a replicação dos dados retidos para a nuvem pública; 6. Deve ser fornecida com discos rígidos hot-pluggable e hot-swappable, permitindo substituição sem necessidade interrupção do funcionamento da solução; 7. Deve ser entregue com arranjos de discos rígidos do tipo RAID-6 ou RAID-DP, configurado de tal modo a tolerar a falha de até 2 (dois) discos rígidos e contar com ao menos 1 disco de hot-spare para cada RAID group, para os discos destinados ao armazenamento de dados de backup; 8. Deve permitir montagem em rack padrão 19" do CLIENTE e deve ser entregue com todos os trilhos, cabos, conectores, manuais de operação e quaisquer outros componentes que sejam necessários à instalação, customização e plena operação; 9. Deve possuir, no mínimo, 70 TB (setenta terabytes) úteis sem considerar taxa de deduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento; 10. Deve suportar a expansão de sua capacidade para, no mínimo, 450TB (quatrocentos e cinquenta terabytes) de capacidade líquida (sem considerar taxas de deduplicação, compressão, perdas com formatação e área necessária para o sistema do equipamento). Esta ampliação de capacidade deverá ser realizada através de unidades de expansão, para o mesmo conjunto de armazenamento, mantendo a característica de deduplicação global da solução; 11. Deve possuir pelo menos 2 (duas) interfaces de rede 10 GbE (dez Gigabit Ethernet) para conexão com switch LAN (interconnect) por meio de conector óptico (SFP+) para Backups executados via LAN. Os conectores devem ser fornecidos em conjunto com o equipamento, bem como 2 (dois) cabos DAC de 3 metros compatível com o switch existente. 13. Deve possuir pelo menos 2 (duas) interfaces de rede 1 GbE (um Gigabit Ethernet) para conexão com switch LAN (interconnect) por meio de conector UTP CAT6 para gerenciamento. Os conectores devem ser fornecidos em conjunto com o equipamento; 14. Deve possuir pelo menos 1 (um) Porta IPMI/iLO/iDRAC ou similar; 15. Deve possuir taxa de transferência de, no mínimo, 7 TB/hora (sete terabytes por hora) para operações de backup desconsiderando qualquer ganho com compressão e deduplicação na origem (cliente e servidor de backup). 16. Deve ser novo, de primeiro uso, da linha de equipamentos (modelos) mais recentemente anunciada pelo fabricante, estar em linha de fabricação e não ter previsão de EOSL (end of Service life)	UNIDADE	3	745.295,29	2.235.885,87

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	anunciada para os próximos 5 anos na data da abertura da licitação; 17. Deve constar no site do fabricante (documento oficial e público) como um appliance ou sistema de armazenamento de backup em disco, em linha de produção; 18. Não serão aceitas soluções montadas especificamente para esse certame, composições de soluções em regime de OEM, nem equipamentos usados, remanufaturados, de demonstração ou gateways. ----- SOFTWARE CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. Deve ser homologado e plenamente compatível com o software de proteção existente do fabricante Veeam (utilizado pelo IFSC). 2. Deve corresponder a um sistema inteligente de armazenamento de backup em disco, que se entende como um subsistema com o propósito específico de armazenamento de backup com compactação, deduplicação e replicação dos dados deduplicados; 3. Não serão aceitas soluções definidas por Software (Virtual Appliance); 4. Deve permitir a utilização de todas as funcionalidades, tecnologias e recursos especificados, de maneira perpétua, irrestrita e sem necessidade de licenciamentos ou ônus adicionais, já licenciados para a capacidade máxima ofertada no certame; 5. Todas as licenças de software necessárias para o completo atendimento das especificações técnicas dos equipamentos deverão ser ofertadas na modalidade de uso perpétuo, ou seja, os equipamentos deverão continuar a operar normalmente mesmo após o período de manutenção e assistência técnica contratado, e deverão ser fornecidas na capacidade máxima suportada pelos equipamentos. 6. O sistema ofertado deverá possuir uma arquitetura do tipo "scale-up" ou do tipo "scale-out" assegurando escalabilidade vertical ou horizontal. Consequentemente, não serão aceitas ofertas de sistemas baseados em federação ou cluster de equipamentos de menor porte, se o conjunto do repositório de armazenamento não for capaz de efetuar deduplicação global dos dados retidos entre os dispositivos. Gateways ou composições desenvolvidas e fabricadas exclusivamente para fins de atendimento do objeto do edital não serão aceitas em hipótese alguma. 7. O sistema de armazenamento fornecido deve permitir a adição futura de ao menos mais uma controladora (nó de processamento) no mesmo conjunto de armazenamento para atuar em modo de alta-disponibilidade ativo-passivo (failover) ou ativo-ativo (load-balance) para as tarefas de backup, de forma que na eventualidade da falha de uma das controladoras (nó de processamento), as atividades de backup possam ser automaticamente redirecionadas para a outra controladora; 8. Deve ser agnóstico ao software de backup, sendo, no mínimo, compatível com os softwares Veritas Netbackup, IBM Spectrum Protect (TSM), Veeam Backup & Recovery, DELL EMC NetWorker e Commvault, garantindo total integração; 9. Possuir mecanismos que protejam contra a inconsistência dos dados mesmo em casos de interrupção abrupta ou desligamento acidental; 10. Deverá implementar mecanismos de validação da consistência dos dados deduplicados armazenados, garantindo que eles estejam íntegros durante backups, restaurações e replicações. A tecnologia deverá reparar, automaticamente, dados que não estejam consistentes com as rotinas executadas. O mecanismo deve ser nativo do equipamento, não sendo aceitos scripts para atendimento deste item; 11. Deve possuir funcionalidade de deduplicação dos dados em nível de bloco ou bytes, com capacidade de eliminação de dados redundantes para racionalizar a utilização do espaço de armazenamento. Serão aceitas soluções que efetuem a deduplicação em linha (inline) ou em paralelo. Caso possua deduplicação em linha (inline), deve fornecer todo o licenciamento e componentes para ativar essa funcionalidade em toda a volumetria útil entregue. Não serão aceitas soluções que efetuem deduplicação post-processing, requerendo janela de deduplicação, nem limitando a execução de backups, restores e replicações durante a execução do processo de deduplicação; 12. Deve suportar que a deduplicação seja realizada juntamente com as operações de backup e restauração, tornando desnecessária uma janela dedicada para sua execução; 13. Deve possuir deduplicação global, mesmo que o armazenamento esteja dividido em volumes lógicos, sendo capaz de identificar dados duplicados de backups de diferentes origens dentro de um mesmo sistema de modo a maximizar a taxa de deduplicação e garantindo que os dados retidos sejam gravados uma única vez; 14. Deve suportar simultaneamente acessos de leitura e gravação pelos protocolos CIFS, NFS e OST; 15. Deve permitir a execução de processos de backup e restore em paralelo; 16. Deve possuir interface WEB para gerenciamento do sistema de armazenamento de backup; 17. Deve possuir integração com o Microsoft Active Directory 2012 e superiores, para autenticação e definição de perfis de acesso. Deve ainda permitir a configuração de duplo fator de autenticação para acesso ao gerenciamento do sistema via integração com sistemas de senha descartável (senha de uso único, em inglês: One-time password - OTP), tais como Google Authenticator, Microsoft Authenticator ou similares. Caso o equipamento requiera um dispositivo/sistema OTP específico e este necessite de licenciamento, hardwares e/ou infraestrutura próprios (ex. Common Access Card (CAC)/Personal Information Verification (PIV) cards, etc.), o mesmo deve ser fornecido em conjunto (hardwares, softwares, licenças, serviços, etc.) para, no				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	mínimo, 5 usuários; 18. Deve possuir funcionalidade para replicação de backups em site remoto de forma assíncrona entre subsistemas semelhantes do mesmo fabricante, utilizando recursos de desduplicação, permitindo reduzir o consumo do link de comunicação. Essa funcionalidade deve ser suportada pelo mesmo fabricante do subsistema e deve ser entregue licenciada para toda a capacidade fornecida; 19. Deve permitir replicar os dados através de rede IP (WAN/LAN); 20. Deve estar licenciado para replicar todo o sistema de armazenamento de backup, incluindo a capacidade de expansão; Deve permitir que as aplicações Oracle (RMAN) e Microsoft SQL realizem backups do tipo Stream Based (Oracle Stream Backup) e "database dump" diretamente para o equipamento, via CIFS e NFS, sem utilizar o software de backup para evitar, assim, o consumo de suas licenças e sem a necessidade de licenciar os volumes (TBs) ou os servidores de banco de dados (CPU, Tier, Core) junto ao software de backup. Se houver necessidade de licenciar essa funcionalidade no equipamento ofertado, todas as licenças necessárias devem ser inclusas; 21. Deve possuir recursos avançados de cibersegurança para prevenção de ataques cibernéticos do tipo Ransomware garantindo a proteção dos dados retidos, com as seguintes características: 21.1. Tal proteção deve ser do dispositivo de armazenamento ofertado e deverá funcionar de maneira automática e transparente, isto é, independentemente do software/utilitário de backup, sem depender do desenvolvimento de scripts de integração e sem requerer ações ou atividades manuais sobre o dado retido; 21.2. Deve garantir a inviolabilidade (imutabilidade) dos dados retidos, garantindo assim que os dados protegidos não possam ser alterados ou apagados, mesmo se o software de backup ou ambiente operacional onde ele opera ficar sob controle do atacante (hacker, malware). Tal proteção deve garantir que, mesmo nas situações em que o atacante procure expirar o conteúdo dos backups através do catálogo do software de backup, os dados retidos ainda possam ser recuperados por um período de dias; 21.3. Não pode requerer e nem ser recomendada janela específica para a aplicação do recurso de proteção dos dados retidos, considerando o conjunto do Software de Backup envolvido e Equipamento ofertado, ou seja, a proteção deverá ser aplicada de forma imediata, assim que os dados retidos sejam desduplicados; 21.4. Deve fazer uso do conceito de isolamento para a proteção dos dados, ou seja, os dados protegidos deverão estar invisíveis da superfície de ataque, isto é, não poderão ser acessados através da rede nem pelo software/utilitário de backup. 21.5. Possuir recurso de dupla autorização (Dual Authorization – Dual Auth), ou seja, alterações das configurações contra Ransomware deverão ser aprovadas por um segundo usuário; 22. Todos os componentes necessários (hardware, software, licenciamento, serviços etc.) para a proteção dos dados de backup devem ser fornecidos em conjunto com a solução e devem manter as condições de escalabilidade e desempenho especificadas nesse projeto; 23. Deve possuir recursos para monitoramento remoto pelo fabricante, tal como notificação do tipo CallHome, para verificação proativa de componentes de hardware em situação de falha ou pré-falha; 24. Deve possuir suporte aos protocolos de monitoramento SNMP e Syslog; ----- SUPORTE E GARANTIA CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. A CONTRATADA deverá fornecer juntamente com a solução de armazenamento de backup acesso a um engenheiro de suporte nomeado de 2º nível do fabricante (nível onde o analista de suporte é qualificado para atuar diretamente no problema, sem necessidade de triagem prévia), que atuará como ponto único de contato para fornecer assistência avançada de forma remota em horário comercial. Caso este engenheiro de suporte esteja temporariamente indisponível, deve ser dado a opção de o caso ser redirecionado para um outro engenheiro de suporte também de 2º nível. O engenheiro de suporte do fabricante deve, adicionalmente, realizar durante todo o período de garantia as seguintes atividades: atualização da solução de armazenamento de backup, verificações proativas junto ao CONTRATANTE, esclarecimento de dúvidas técnicas e apoio em atividades de revisão e alteração de configurações do dia a dia. 2. Caso a CONTRATADA não consiga atender ao nível de suporte exigido com recurso nomeado de 2º nível, será aceito o fornecimento de serviços na modalidade remoto como forma de atendimento, desde que seja do próprio fabricante e seja disponibilizado recurso humano certificado tecnicamente na solução no qual será ponto único de contato para todas as questões relacionadas a suporte técnico, incluindo abertura e acompanhamento de ponta-a-ponta dos casos de suporte, assim como das demais atividades listadas. 3. Durante a vigência da garantia, deverão ser instaladas, sem custos adicionais, todas as atualizações, alterações e melhorias introduzidas nos softwares objetos da presente contratação imediatamente a sua homologação e publicação, buscando assim garantir que a solução esteja nas conformidades recomendadas pelo fabricante, desde que compatíveis com o equipamento adquirido; 4. O atendimento de suporte remoto do fabricante deve permitir, sem limite de quantidade, durante a vigência da garantia, que o suporte remoto realize, pelo menos, as seguintes tarefas: instalação de correções e atualizações, revisão das configurações e sugestão de melhores práticas do				

Item	Descrição	Unidade	Quant.	Preço Unit. (R\$)	Valor Total (R\$)
	fabricante, reconfiguração e reinstalação do appliance, quando for necessário; 5. Deve ser ofertado garantia e suporte técnico para a solução por um período mínimo de 3 anos. ----- SERVIÇO DE INSTALAÇÃO (HARDWARE, SOFTWARE E GARANTIA) CARACTERÍSTICAS MÍNIMAS OBRIGATÓRIAS: 1. Deverá ser feita a montagem em rack padrão 19", alimentação elétrica e conexão do equipamento à rede de dados. 2. O serviço de instalação consiste na colocação do equipamento em pleno funcionamento, em conformidade com o disposto nesta especificação técnica, no Edital e seus Anexos e em perfeitas condições de operação, de forma integrada ao ambiente de infraestrutura de informática da Contratante e deve contemplar, no mínimo, o seguinte: 2.1. Montagem em rack padrão 19" indicado pela contratante, alimentação elétrica e conexão do equipamento à rede de dados; 2.2. Conexão e configuração do appliance de backup no switch de rede do Contratante; 2.3. Atualização de softwares, firmwares e drives que compõem a solução; 2.4. Instalação, configuração e aplicação das licenças aplicáveis; 2.5. Documentação do ambiente configurado e instalado. 2.6. A ativação e configuração da solução deve ser realizada segundo as boas práticas do fabricante, disponibilizando o appliance de backup em condições de pleno funcionamento.				
Valor Total do Lote/Grupo: R\$ 3.496.854,05					

Valor Total do Processo: R\$ 10.646.626,12

SIPAC DTIC - Diretoria de Tecnologia da Informação e Comunicação - (48) 3877-9000 Copyright © 2005-2024 - UFRN - appdocker3-srv1,appdocker3-inst1



ATA DE REGISTRO DE PREÇOS

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

ATA DE REGISTRO DE PREÇOS

N.º

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, com sede na cidade de Florianópolis/Estado de Santa Catarina, inscrito no CNPJ sob o nº 11.402.887/0001-60, neste ato representado pelo seu Reitor, Maurício Gariba Júnior, nomeado pelo Decreto de 09 de agosto de 2021, publicado no DOU 10 de agosto de 2021, Edição 150, Seção 2, página 1, portador da Matrícula Funcional nº 0277933, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº/202..., publicada no de/...../202....., processo administrativo nº 23292.034402/2023-70, RESOLVE registrar os preços da(s) empresa(s) indicada(s) e qualificada(s) nesta ATA, de acordo com a classificação por ela(s) alcançada(s) e na(s) quantidade(s) cotada(s), atendendo as condições previstas no **Edital de licitação**, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto nº 11.462, de 31 de março de 2023, e em conformidade com as disposições a seguir:

1. DO OBJETO

- 1.1. A presente Ata tem por objeto o registro de preços para a eventual contratação de EQUIPAMENTOS DE SEGURANÇA DE TI, especificado no item 1.1 Termo de Referência, anexo I do edital de Licitação nº 31009/2023, 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 de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item do TR	Fornecedor (<i>razão social, CNPJ/MF, endereço, contatos, representante</i>)						
X	Especificação	Marca (se exigida no edital)	Modelo (se exigido no edital)	Unidade	Quantidade	Valor Un	Prazo garantia ou validade

- 2.2. A listagem do cadastro de reserva referente ao presente registro de preços consta como anexo a esta Ata.

3. ÓRGÃO(S) GERENCIADOR E PARTICIPANTE(S)

- 3.1. O órgão gerenciador será o Instituto Federal de Santa Catarina - IFSC



3.2. *Não há participantes cadastrados na IRP da presente licitação.*

4. DA ADESÃO À ATA DE REGISTRO DE PREÇOS

- 4.1. Durante a vigência da ata, os órgãos e as entidades da Administração Pública federal, estadual, distrital e municipal que não participaram do procedimento de IRP poderão aderir à ata de registro de preços na condição de não participantes, observados os seguintes requisitos:
- 4.1.1. apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
 - 4.1.2. demonstração de que os valores registrados estão compatíveis com os valores praticados pelo mercado na forma do art. 23 da Lei nº 14.133, de 2021; e
 - 4.1.3. consulta e aceitação prévias do órgão ou da entidade gerenciadora e do fornecedor.
- 4.2. A autorização do órgão ou entidade gerenciadora apenas será realizada após a aceitação da adesão pelo fornecedor.
- 4.2.1. O órgão ou entidade gerenciadora poderá rejeitar adesões caso elas possam acarretar prejuízo à execução de seus próprios contratos ou à sua capacidade de gerenciamento.
- 4.3. Após a autorização do órgão ou da entidade gerenciadora, o órgão ou entidade não participante deverá efetivar a aquisição ou a contratação solicitada em até noventa dias, observado o prazo de vigência da ata.
- 4.4. O prazo de que trata o subitem anterior, relativo à efetivação da contratação, poderá ser prorrogado excepcionalmente, mediante solicitação do órgão ou da entidade não participante aceita pelo órgão ou pela entidade gerenciadora, desde que respeitado o limite temporal de vigência da ata de registro de preços.
- 4.5. O órgão ou a entidade poderá aderir ao item da ata de registro de preços da qual seja integrante, na qualidade de não participante, para aqueles itens para os quais não tenha quantitativo registrado, observados os requisitos do item 4.1.

Dos limites para as adesões

- 4.6. As aquisições ou contratações adicionais não poderão exceder, por órgão ou entidade, a cinquenta por cento dos quantitativos dos itens do instrumento convocatório registrados na ata de registro de preços para o gerenciador e para os participantes.
- 4.7. O quantitativo decorrente das adesões não poderá exceder, na totalidade, ao dobro do quantitativo de cada item registrado na ata de registro de preços para o gerenciador e os participantes, independentemente do número de órgãos ou entidades não participantes que aderirem à ata de registro de preços.
- 4.8. A adesão à ata de registro de preços por órgãos e entidades da Administração Pública estadual, distrital e municipal poderá ser exigida para fins de transferências voluntárias, não ficando sujeita ao limite de que trata o item 4.7, desde que seja destinada à execução descentralizada de programa ou projeto federal e comprovada a compatibilidade dos preços registrados com os valores praticados no mercado na forma do art. 23 da Lei nº 14.133, de 2021.



Vedação a acréscimo de quantitativos

4.9. É vedado efetuar acréscimos nos quantitativos fixados na ata de registro de preços.

5. VALIDADE, FORMALIZAÇÃO DA ATA DE REGISTRO DE PREÇOS E CADASTRO RESERVA

5.1. A validade da Ata de Registro de Preços será de 1 (um) ano, 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 ou da contratação direta, 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, devendo ser observada a possibilidade de o licitante oferecer ou não proposta em quantitativo inferior ao máximo previsto **no edital** e se obrigar nos limites dela;

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, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e

5.4.2.2. Mantiverem sua proposta original.

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

5.5. 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.

5.6. 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.

5.7. A habilitação dos licitantes que comporão o cadastro de reserva a que se refere o item 5.4.2.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:



- 5.7.1. Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos *no edital*; e
- 5.7.2. Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.
- 5.8. 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.
- 5.9. Após a homologação da licitação ou da contratação direta, o licitante mais bem classificado ou o fornecedor, no caso da contratação direta, 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.
- 5.9.1. 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. 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 5.7, observando o item 5.7 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 trata o item 5.4.2.1, 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 de cláusula de reajustamento ou repactuação sobre os preços registrados, nos termos da Lei nº 14.133, de 2021.

6.1.3.1. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;

6.1.3.2. No caso da repactuação, poderá ser a pedido do interessado, conforme critérios definidos para a contratação.

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 diligenciar 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. Não 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 9.1, 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 5.7.

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 9.4, 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 7.2 e no item 7.2.1, 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 e não 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; ou

8.2.2. De órgão ou entidade participante para órgão ou entidade não 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. Na hipótese de remanejamento de órgão ou entidade participante para órgão ou entidade não participante, serão observados os limites previstos no art. 32 do Decreto nº 11.462, de 2023.

8.5. Competirá ao órgão ou à entidade gerenciadora autorizar o remanejamento solicitado, com a redução do quantitativo inicialmente informado pelo órgão ou pela entidade participante, desde que haja prévia anuência do órgão ou da entidade que sofrer redução dos quantitativos informados.

8.6. Caso o remanejamento seja feito entre órgãos ou entidades dos Estados, do Distrito Federal ou de Municípios distintos, caberá ao fornecedor beneficiário da ata de registro de preços, observadas as condições nela estabelecidas, optar pela aceitação ou não do fornecimento decorrente do remanejamento dos itens.

8.7. Na hipótese da compra centralizada, não havendo indicação pelo órgão ou pela entidade gerenciadora, dos quantitativos dos participantes da compra centralizada, nos termos do item 8.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.



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.
 - 9.1.4.1. 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.
- 9.2. 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.
- 9.3. 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.
- 9.4. 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:
 - 9.4.1. Por razão de interesse público;
 - 9.4.2. A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou
 - 9.4.3. Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos do 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 para entrega 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. *No caso de adjudicação por preço global de grupo de itens, só será admitida a contratação de parte de itens do grupo se houver prévia pesquisa de mercado e demonstração de sua vantagem para o órgão ou a entidade.*

Para firmeza e validade do pactuado, a presente Ata foi lavrada em via digital, que, depois de lida e achada em ordem, vai assinada pelas partes por meio da declaração de concordância à Ata de Registro de Preços.

Local e data

Assinaturas

Representante legal do órgão gerenciador e representante(s) legal(is) do(s) fornecedor(s)
registrado(s)



MODELO

DECLARAÇÃO DE CONCORDÂNCIA À ATA DE REGISTRO DE PREÇOS
PREGÃO ELETRÔNICO (SRP) 31009/2023 – IFSC

A empresa _____

declara para os devidos fins, que:

1. Recebeu a Ata de Registros de Preços do Pregão Eletrônico nº XX/20XX do IFSC, contendo _____ páginas (incluindo Ata e anexos) e;
2. Concorda com todos os termos da referida Ata e o Anexo I, com os preços registrados.
3. Assume o compromisso de receber as Autorizações de Fornecimento e Empenhos pelo e-mail institucional (e-mail da empresa @.....) Concordando que não sendo confirmado o recebimento do e-mail, o IFSC considerará como recebido, iniciando a contagem do prazo de entrega. Assumindo o compromisso de avisar o IFSC quando houver mudança do e-mail

_____, ____ de _____ de 20XX.

(assinatura e identificação do Representante
Legal e Carimbo da Empresa

Anexo

Cadastro Reserva

Seguindo a ordem de classificação, segue relação de fornecedores que aceitaram cotar os itens com preços iguais ao adjudicatário:

Item do TR	Fornecedor (<i>razão social, CNPJ/MF, endereço, contatos, representante</i>)							
X	Especificação	Marca (se exigida no edital)	Modelo (se exigido no edital)	Unidade	Quantidade Máxima	Quantidade de Mínima	Valor Un	Prazo garantia ou validade

Seguindo a ordem de classificação, segue relação de fornecedores que mantiveram sua proposta original:

Item do TR	Fornecedor (<i>razão social, CNPJ/MF, endereço, contatos, representante</i>)							
X	Especificação	Marca (se exigida no edital)	Modelo (se exigido no edital)	Unidade	Quantidade Máxima	Quantidade de Mínima	Valor Un	Prazo garantia ou validade

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA

(Processo Administrativo nº 23292.034402/2023-70)

CONTRATO ADMINISTRATIVO Nº/....., QUE FAZEM
ENTRE SI A UNIÃO, POR INTERMÉDIO DO (A)
..... E
.....

O INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SANTA CATARINA, com sede na cidade de Florianópolis/Estado de Santa Catarina, inscrito no CNPJ sob o nº 11.402.887/0001-60, neste ato representado pelo seu Reitor, Maurício Gariba Júnior, nomeado pelo Decreto de 09 de agosto de 2021, publicado no DOU 10 de agosto de 2021, Edição 150, Seção 2, página 1, portador da Matrícula Funcional nº 0277933, doravante denominado CONTRATANTE, e o(a), inscrito(a) no CNPJ/MF sob o nº, sediado(a) na, em doravante designado CONTRATADO, neste ato representado(a) por (nome e função no contratado), conforme atos constitutivos da empresa OU procuração apresentada nos autos, tendo em vista o que consta no Processo nº e em observância às disposições da Lei nº 14.133, de 1º de abril de 2021, e demais legislação aplicável, resolvem celebrar o presente Termo de Contrato, decorrente do Pregão Eletrônico n.21101/2023, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO (art. 92, I e II)

- 1.1. O objeto do presente instrumento é a contratação de solução de tecnologia da informação e comunicação composta por AQUISIÇÃO DE EQUIPAMENTOS DE SEGURANÇA DE TI, nas condições estabelecidas no Termo de Referência.
- 1.2. Este instrumento contratual tem por objeto os serviços vinculados aos bens móveis descritos no item 1.3.

São serviços vinculados:

- 1.2.1.1. Entrega dos equipamentos;
- 1.2.1.2. Instalação/configuração dos equipamentos;
- 1.2.1.3. Abertura de chamados - recebimento por parte da contratada;
- 1.2.1.4. Atendimento de um chamado aberto;
- 1.2.1.5. Resolução total de um problema apresentado em um chamado.

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

Os serviços vinculados descritos acima, serão avaliados mediante os instrumentos de medição disponíveis no Termo de Referência.

1.3. Objeto da contratação:

ITEM	ESPECIFICAÇÃO	UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
NÃO ASSOCIADO(S) A LOTE/GRUPO					
01	ADAPTADOR DE TELEFONIA ANALÓGICA COM PORTAS FXS/FXO	UNIDADE	50	928,00	46.400,00
26	SERVIDOR EM LÂMINA	UNIDADE	7	247.316,67	1.731.216,69
38	USER MEDIA GATEWAY - VOIP	UNIDADE	2	3.907,13	7.814,26
LOTE/GRUPO 1: REDE SEM FIO					
05	INJETOR POE – SOLUÇÃO DE GERENCIAMENTO DE REDES E SEGURANÇA	UNIDADE	50	1.510,75	75.537,50
09	PONTO DE ACESSO INDOOR - TIPO I - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	100	6.095,48	609.548,00
10	PONTO DE ACESSO INDOOR - TIPO II - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	40	10.293,39	411.735,60
11	PONTO DE ACESSO OUTDOOR - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	10	11.072,04	110.720,40
20	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO I	UNIDADE	100	1.300,11	130.011,00
21	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT INDOOR TIPO II	UNIDADE	40	2.195,43	87.817,20
22	SERVIÇO DE SUPORTE E GARANTIA ACCESS POINT OUTDOOR	UNIDADE	10	2.361,56	23.615,60
25	SERVIÇO TÉCNICO PARA SITE SURVEY - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	12	9.674,02	116.088,24

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

ITEM	ESPECIFICAÇÃO	UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
LOTE/GRUPO 2: CONEXÃO DE REDE					
23	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 1	UNIDADE	4	6.139,86	24.559,44
24	SERVIÇO DE SUPORTE E GARANTIA SWITCH CORE - TIPO 2	UNIDADE	4	8.863,76	35.455,04
31	SWITCH CORE - TIPO 1 – SOLUÇÃO DE SEGURANÇA DADOS	UNIDADE	4	28.677,61	114.710,44
32	SWITCH CORE - TIPO 2 – SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	4	41.400,18	165.600,72
33	SWITCH CORE TIPO 3 – SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	2	164.139,38	328.278,76
34	TRANSCEIVER 10GBASE-LR - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	20	3.377,76	67.555,20
35	TRANSCEIVER 10GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	20	1.196,15	23.923,00
36	TRANSCEIVER 40GBASE-SR - SOLUÇÃO DE SEGURANÇA DE DADOS	UNIDADE	10	30.930,54	309.305,40
LOTE/GRUPO 3: SEGURANÇA DE REDE					
04	FONTE HOT SWAPPABLE - FORTIGATE 600E	UNIDADE	4	8.773,50	35.094,00
06	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE 60F	UNIDADE	6	12.505,08	75.030,48
07	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-100F	UNIDADE	1	42.246,77	42.246,77
08	LICENÇAS DE PROTEÇÃO UNIFICADA CONTRA AMEAÇAS PARA O FIREWALL FORTIGATE-80F	UNIDADE	5	21.545,87	107.729,35



TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

12	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3	UNIDADE	16	10.084,63	161.354,08
ITEM	ESPECIFICAÇÃO	UNIDADE	QTDE	VALOR UNITÁRIO (R\$)	VALOR TOTAL (R\$)
13	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4	UNIDADE	5	11.148,61	55.743,05
14	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5	UNIDADE	4	11.762,52	47.050,08
15	SERVIÇO DE CONFIGURAÇÃO - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6	UNIDADE	2	13.716,78	27.433,56
16	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 3	UNIDADE	16	20.446,53	327.144,48
17	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 4	UNIDADE	5	40.091,21	200.456,05
18	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 5	UNIDADE	4	74.088,60	296.354,40
19	SERVIÇO DE SUPORTE E GARANTIA - SOLUÇÃO SEGURANÇA DE DADOS - TIPO 6	UNIDADE	2	202.947,00	405.894,00
27	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 3	UNIDADE	16	14.395,43	230.326,88
28	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 4	UNIDADE	05	28.226,36	141.131,80
29	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 5	UNIDADE	4	52.162,32	208.649,28
30	SOLUÇÃO DE SEGURANÇA DE DADOS - TIPO 6	UNIDADE	2	180.481,52	360.963,04

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

37	TREINAMENTO – SOLUÇÃO DE SEGURANÇA DE DADOS	SERVIÇO	1	7.278,28	7.278,28
LOTE/GRUPO 4: BACKUP DE DADOS					
2	APPLIANCE DE BACKUP - TIPO 1	UNIDADE	2	630.484,09	1.260.968,18
3	APPLIANCE DE BACKUP - TIPO 2	UNIDADE	2	745.295,29	1.490.590,58
VALOR TOTAL				R\$ 9.901.330,83	

1.1.

1.4. Vinculam esta contratação, independentemente de transcrição:

- O Termo de Referência;
- O Edital da Licitação;
- A Proposta do contratado;
- Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1. O prazo de vigência da contratação estará vinculado ao período de garantia dos bens que serão adquiridos, de acordo com o exposto no Termo de Referência, a saber:

- 1 (um) ano para os **itens 1 e 38**;
- 3 (três) anos para os demais itens.

2.2. Não haverá prorrogação de contrato.

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS (art. 92, IV, VII e XVIII)

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

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1. Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA - PREÇO

5.1. O valor da execução dos serviços de instalação/configuração, bem como os serviços de suporte e garantia estão definidos como valores únicos não havendo ônus contínuo (mensal) para o IFSC.

5.2. No valor do equipamento estão incluídas todas as despesas ordinárias diretas e indiretas decorrentes da execução do objeto, inclusive tributos e/ou impostos, encargos sociais,

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

trabalhistas, previdenciários, fiscais e comerciais incidentes, taxa de administração, frete, seguro e outros necessários ao cumprimento integral do objeto da contratação.

CLÁUSULA SEXTA - PAGAMENTO (art. 92, V e VI)

- 6.1. O prazo para pagamento (bens/serviços) ao contratado e demais condições a ele referentes encontram-se definidos no Termo de Referência, anexo a este Contrato.

CLÁUSULA SÉTIMA - REAJUSTE (art. 92, V)

- 7.1. *Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data da assinatura da Ata de Registro de Preços.*
- 7.2. *Após o interregno de um ano, considerando a renovação da Ata de Registro de Preços, os preços iniciais serão reajustados a pedido da Contratada, mediante a aplicação, pelo contratante, do Índice de Custos de Tecnologia da Informação - ICTI, mantido pela Fundação Instituto de Pesquisa Econômica Aplicada - IPEA, exclusivamente para as obrigações iniciadas e concluídas após a ocorrência da anualidade.*
- 7.3. *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.*
- 7.4. *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.*
- 7.5. *O reajuste será realizado por apostilamento.*

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE (art. 92, X, XI e XIV)

- 8.1. São obrigações do Contratante, além das previstas no termo de referência:

Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos;

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

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

Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;

Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato e no Termo de Referência;

Aplicar ao Contratado as sanções previstas na lei e neste Contrato;

Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado;

Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.

A Administração terá o prazo de *um mês*, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.

Responder eventuais pedidos de restabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de *dois meses*.

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

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

CLÁUSULA NONA - OBRIGAÇÕES DO CONTRATADO (art. 92, XIV, XVI e XVII)

- 9.1. O Contratado deve cumprir todas as obrigações constantes deste Contrato e em seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:

Entregar o objeto acompanhado do manual do usuário, com uma versão em português ou inglês, e a relação da rede de assistência técnica autorizada;

Responsabilizar-se pelos vícios e danos decorrentes do objeto, de acordo com o Código de Defesa do Consumidor ([Lei nº 8.078, de 1990](#));

Comunicar ao contratante, no prazo máximo de 24 (vinte e quatro) horas que antecede a data da entrega, os motivos que impossibilitem o cumprimento do prazo previsto, com a devida comprovação;

Atender às determinações regulares emitidas pelo fiscal ou gestor do contrato ou autoridade superior ([art. 137, II, da Lei n.º 14.133, de 2021](#)) e prestar todo esclarecimento ou informação por eles solicitados;

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

Responsabilizar-se pelos vícios e danos decorrentes da execução do objeto, bem como por todo e qualquer dano causado à Administração ou terceiros, não reduzindo essa responsabilidade a fiscalização ou o acompanhamento da execução contratual pelo contratante, que ficará autorizado a descontar dos pagamentos devidos ou da garantia, caso exigida, o valor correspondente aos danos sofridos;

Quando não for possível a verificação da regularidade no Sistema de Cadastro de Fornecedores – SICAF, o contratado deverá entregar ao setor responsável pela fiscalização do contrato, junto com a Nota Fiscal para fins de pagamento, os seguintes documentos: 1) prova de regularidade relativa à Seguridade Social; 2) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União; 3) certidões que comprovem a regularidade perante a

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

Fazenda Estadual ou Distrital do domicílio ou sede do contratado; 4) Certidão de Regularidade do FGTS – CRF; e 5) Certidão Negativa de Débitos Trabalhistas – CNDT;

Responsabilizar-se pelo cumprimento de todas as obrigações trabalhistas, previdenciárias, fiscais, comerciais e as demais previstas em legislação específica, cuja inadimplência não transfere a responsabilidade ao contratante e não poderá onerar o objeto do contrato;

Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal ou acidente que se verifique no local da execução do objeto contratual.

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

Cumprir, durante todo o período de execução do contrato, a reserva de cargos prevista em lei para pessoa com deficiência, para reabilitado da Previdência Social ou para aprendiz, bem como as reservas de cargos previstas na legislação (art. 116, da Lei n.º 14.133, de 2021);

Comprovar a reserva de cargos a que se refere a cláusula acima, no prazo fixado pelo fiscal do contrato, com a indicação dos empregados que preencheram as referidas vagas (art. 116, parágrafo único, da Lei n.º 14.133, de 2021);

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

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

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

A empresa contratada deverá assinar o Termo de Compromisso de Manutenção de Sigilo e o Termo de Ciência da Declaração de Manutenção de Sigilo resguardando que os recursos, dados e informações de propriedade da CONTRATANTE, e quaisquer outros, repassados por força do objeto desta licitação e do contrato, que constituam informação privilegiada e possuem caráter de confidencialidade.

CLÁUSULA DÉCIMA PRIMEIRA– OBRIGAÇÕES PERTINENTES À LGPD

- 10.1. As partes deverão cumprir a Lei nº 13.709, de 14 de agosto de 2018 (LGPD), quanto a todos os dados pessoais a que tenham acesso em razão do certame ou do contrato administrativo que eventualmente venha a ser firmado, a partir da apresentação da proposta no procedimento de contratação, independentemente de declaração ou de aceitação expressa.
- 10.2. Os dados obtidos somente poderão ser utilizados para as finalidades que justificaram seu acesso e de acordo com a boa-fé e com os princípios do art. 6º da LGPD.
- 10.3. É vedado o compartilhamento com terceiros dos dados obtidos fora das hipóteses permitidas em Lei.

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

- 10.4. A Administração deverá ser informada no prazo de 5 (cinco) dias úteis sobre todos os contratos de suboperação firmados ou que venham a ser celebrados pelo Contratado.
- 10.5. 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.
- 10.6. É dever do contratado orientar e treinar seus empregados sobre os deveres, requisitos e responsabilidades decorrentes da LGPD.
- 10.7. O Contratado deverá exigir de suboperadores e subcontratados o cumprimento dos deveres da presente cláusula, permanecendo integralmente responsável por garantir sua observância.
- 10.8. O Contratante poderá realizar diligência para aferir o cumprimento dessa cláusula, devendo o Contratado atender prontamente eventuais pedidos de comprovação formulados.
- 10.9. O Contratado deverá prestar, no prazo fixado pelo Contratante, prorrogável justificadamente, quaisquer informações acerca dos dados pessoais para cumprimento da LGPD, inclusive quanto a eventual descarte realizado.
- 10.10. 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.
- 10.11. Os referidos bancos de dados devem ser desenvolvidos em formato interoperável, a fim de garantir a reutilização desses dados pela Administração nas hipóteses previstas na LGPD.
- 10.12. 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.
- 10.13. Os contratos e convênios de que trata o § 1º do art. 26 da LGPD deverão ser comunicados à autoridade nacional.

CLÁUSULA DÉCIMA PRIMEIRA– GARANTIA DE EXECUÇÃO (art. 92, XII)

- 11.1. *Não haverá exigência de garantia contratual da execução.*

CLÁUSULA DÉCIMA PRIMEIRA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (art. 92, XIV)

- 12.1. 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;

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

- 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](#).
 - i) *Não atender os prazos estipulados no Termo de Referência para os serviços vinculados.*
- 12.2. 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”, “d” e “i” 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”, “d” e “i”, que justifiquem a imposição de penalidade mais grave ([art. 156, §5º, da Lei nº 14.133, de 2021](#)).
 - iv. **Multa:**
 - 1. moratória de 1% (*um por cento*) por dia de atraso injustificado sobre o valor unitário licitado do bem ao qual foi acionada a garantia, até o limite de 10 (dez) dias;
 - 2. Compensatória, para as infrações descritas nas alíneas “e” a “h” do subitem 11.1, de 2% a 5% do valor do Contrato;
 - 3. Compensatória, para a inexecução total do contrato prevista na alínea “c” do subitem 11.1, de 3% a 6% do valor do Contrato.
 - 4. Para infração descrita na alínea “b” do subitem 11.1, a multa será de 4% a 7% do valor do Contrato.
 - 5. Para infrações descritas na alínea “d” do subitem 11.1, a multa será de 5% a 8% do valor do Contrato.
 - 6. Para a infração descrita na alínea “a” do subitem 11.1, a multa será de 5% a 8% do valor do Contrato, ressalvadas as seguintes infrações:
 - i. Para a infração descrita na alínea “i” do subitem 11.1, a multa será a descrita no termo de referência, nos instrumentos de medição.
- 12.3. 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](#))
- 12.4. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa ([art. 156, §7º, da Lei nº 14.133, de 2021](#)).

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

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](#))

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](#)).

Previamente ao encaminhamento à cobrança judicial, a multa poderá ser recolhida administrativamente no prazo máximo de 30 (*trinta*) dias, a contar da data do recebimento da comunicação enviada pela autoridade competente.

- 12.5. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa ao Contratado, 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.
- 12.6. 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.
- 12.7. 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](#)).
- 12.8. 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](#)).
- 12.9. 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](#)).
- 12.10. 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](#).

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

- 12.11. 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 SEGUNDA– DA EXTINÇÃO CONTRATUAL (art. 92, XIX)

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

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

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.

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

Nesta hipótese, aplicam-se também os [artigos 138 e 139 da mesma Lei](#).

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

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

- 13.4. O termo de extinção, sempre que possível, será precedido:

Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

Relação dos pagamentos já efetuados e ainda devidos;

Indenizações e multas.

- 13.5. A extinção do contrato não configura óbice para o reconhecimento do desequilíbrio econômico-financeiro, hipótese em que será concedida indenização por meio de termo indenizatório ([art. 131, caput, da Lei n.º 14.133, de 2021](#)).

- 13.6. O contrato poderá ser extinto caso se constate que o contratado mantém vínculo de natureza técnica, comercial, econômica, financeira, trabalhista ou civil com dirigente do órgão ou entidade contratante ou com agente público que tenha desempenhado função na licitação ou atue na fiscalização ou na gestão do contrato, ou que deles seja cônjuge, companheiro ou parente em linha reta, colateral ou por afinidade, até o terceiro grau (art. 14, inciso IV, da Lei n.º 14.133, de 2021).

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

CLÁUSULA DÉCIMA TERCEIRA – DOTAÇÃO ORÇAMENTÁRIA (art. 92, VIII)

14.1. As despesas decorrentes da presente contratação correrão à conta de recursos específicos consignados no Orçamento Geral da União deste exercício, na dotação abaixo discriminada:

- I. Gestão/Unidade: 158516;
- II. Fonte de Recursos: 1000000000;
- III. Programa de Trabalho: 171270;
- IV. Elemento de Despesa: 449052;
- V. Plano Interno: L20RLP01CTN;

CLÁUSULA DÉCIMA QUARTA – DOS CASOS OMISSOS (art. 92, III)

15.1. 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 QUINTA – ALTERAÇÕES

- 16.1. Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei nº 14.133, de 2021.
- 16.2. 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.
- 16.3. 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).
- 16.4. Registros que não caracterizam alteração do contrato podem ser realizados por simples apostila, dispensada a celebração de termo aditivo, na forma do art. 136 da Lei nº 14.133, de 2021.

CLÁUSULA DÉCIMA SEXTA – PUBLICAÇÃO

17.1. Incumbirá ao contratante divulgar o presente instrumento no Portal Nacional de Contratações Públicas (PNCP), na forma prevista no art. 94 da Lei 14.133, de 2021, bem como no respectivo sítio oficial na Internet, em atenção ao art. 91, caput, da Lei nº 14.133, de 2021, e ao art. 8º, §2º, da Lei nº 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto nº 7.724, de 2012.

CLÁUSULA DÉCIMA SÉTIMA – FORO (art. 92, §1º)

18.1. Fica eleito o Foro da Justiça Federal em, Seção Judiciária de..... para dirimir os litígios que decorrerem da execução deste Termo de Contrato que não puderem ser compostos pela conciliação, conforme art. 92, §1º, da Lei nº 14.133/21.

TERMO DE CONTRATO ADMINISTRATIVO Nº XXXX/XXXX

[Local], [dia] de [mês] de [ano].

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-

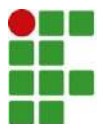


ORDEM DE FORNECIMENTO DE BENS

INTRODUÇÃO
Por intermédio da Ordem de Fornecimento de Bens (OFB) será solicitado formalmente à Contratada o fornecimento de bens relativos ao objeto do contrato. O encaminhamento das demandas deverá ser planejado visando a garantir que os prazos para entrega final de todos os bens e serviços estejam compreendidos dentro do prazo de vigência contratual. Referência: Art. 32 IN SGD Nº 94/2022.

1 – IDENTIFICAÇÃO			
Nº da OS/OFB	xxxx/aaaa	Data de emissão	<dd/mm/aaaa>
CONTRATO/NOTA DE EMPENHO nº	xx/aaaa		
Objeto do Contrato	<Descrição do objeto do contrato>		
Contratada	<Nome da contratada>	CNPJ	99.999.999/9999-99
Preposto	<Nome do preposto>		
Início vigência	<dd/mm/aaaa>	Fim vigência	<dd/mm/aaaa>
ÁREA REQUISITANTE			
Unidade	< Sigla – Nome da unidade>		
Solicitante	<Nome do solicitante>	E-mail	xxxxxxxxxxxxxx

2 – ESPECIFICAÇÃO DOS BENS/SERVIÇOS E VOLUMES ESTIMADOS					
Item	Descrição do bem ou serviço	Métrica	Valor unitário (R\$)	Qtde/Vol.	Valor Total (R\$)
1	...	...	...	...	...
...	...	...	...	...	...
Valor total estimado da OS/OFB					



3 – <INSTRUÇÕES/ESPECIFICAÇÕES> COMPLEMENTARES

<Incluir instruções complementares à execução da OS/OFB>

<Ex.: Contatar a área solicitante para agendamento do horário de entrega>

<Ex.: Conforme consta no Termo de Referência, o recebimento provisório está condicionado à entrega do código no ambiente de homologação, e a documentação do software no repositório oficial de gestão de projetos>

4 – DATAS E PRAZOS PREVISTOS

Data de Início:	<dd/mm/aaaa>	Data do Fim:	<dd/mm/aaaa>
-----------------	--------------	--------------	--------------

CRONOGRAMA DE EXECUÇÃO/ENTREGA

Item	Tarefa/entrega	Início	Fim
1		<dd/mm/aaaa>	<dd/mm/aaaa>
...		<dd/mm/aaaa>	<dd/mm/aaaa>

5 – ARTEFATOS / PRODUTOS

Fornecidos	A serem gerados e/ou atualizados

5 – ASSINATURA E ENCAMINHAMENTO DA DEMANDA

Autoriza-se a <execução dos serviços / entrega dos bens> correspondentes à presente <OS/OFB>, no período e nos quantitativos acima identificados.

<Nome >
**<Responsável pela demanda/
Fiscal Requisitante>**
Matr.: <Nº da matrícula>

<Nome >
Gestor do Contrato
Matr.: <Nº da matrícula>

<Local>, xx de xxxxxxxxx de xxxx



TERMO DE RECEBIMENTO PROVISÓRIO – COMPRAS DE TIC

INTRODUÇÃO

O Termo de Recebimento Provisório declarará, de forma sumária, que as compras foram entregues, para verificação posterior da conformidade do material com as exigências contratuais, baseada nos requisitos e nos critérios de aceitação definidos no Modelo de Gestão do Contrato.

Referência: Inciso XXI, art. 2º, e alínea “i”, inciso II, art. 33 da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO

CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxx
Nº DA OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S) E VOLUMES DE EXECUÇÃO

SOLUÇÃO DE TIC

<Descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>

ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE
1	<Descrição igual ao da OFB de abertura>	<Ex.: UNID.>	<n>
...	...	...	...
...	...	...	...
...	...	...	...
TOTAL DE ITENS			

3 – RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “i”, da IN SGD/ME nº 94/2022, por este instrumento ATESTO que os <bem(s)/produto(s)> correspondentes à <OFB> acima identificada, conforme definido no Modelo de Execução do contrato supracitado, foram entregues, estando sujeitos à avaliação específica para verificação do atendimento às demais exigências contratuais, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do contrato.

Ressaltamos que o recebimento definitivo destes <bem(s)/produto(s)> ocorrerá somente após a verificação desses requisitos e das demais condições contratuais, desde que não se observem inconformidades ou divergências quanto às especificações constantes do Termo de Referência e do Contrato acima identificado que ensejem correções por parte da **CONTRATADA**. Por fim, reitera-se que o objeto poderá ser rejeitado, no todo ou em parte, quando estiver em desacordo com o contrato.

4 – ASSINATURA

FISCAL TÉCNICO

<Nome do Fiscal Técnico do Contrato>

Matrícula: xxxxxx

<Local>, <dia> de <mês> de <ano>.



TERMO DE RECEBIMENTO DEFINITIVO

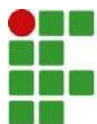
INTRODUÇÃO
O Termo de Recebimento Definitivo declarará formalmente à Contratada que os serviços prestados ou que os bens fornecidos foram devidamente avaliados e atendem às exigências contratuais, de acordo com os requisitos e critérios de aceitação estabelecidos.
Referência: Inciso XXII, Art. 2º e alínea “h” inciso I do art. 33, da IN SGD/ME Nº 94/2022.

1 – IDENTIFICAÇÃO			
CONTRATO/NOTA DE EMPENHO Nº	xx/aaaa		
CONTRATADA	<Nome da Contratada>	CNPJ	xxxxxxxxxxxxx
Nº DA OS/OFB	<xxxx/aaaa>		
DATA DA EMISSÃO	<dd/mm/aaaa>		

2 – ESPECIFICAÇÃO DOS PRODUTO(S)/BEM(S)/SERVIÇOS E VOLUMES DE EXECUÇÃO				
SOLUÇÃO DE TIC				
<descrição da solução de TIC solicitada relacionada ao contrato anteriormente identificado>				
ITEM	DESCRIÇÃO DO BEM OU SERVIÇO	MÉTRICA	QUANTIDADE	TOTAL
1	<descrição igual à da OS/OFB de abertura>	<Ex.: PF>	<n>	<total>
...				
TOTAL DE ITENS				

3 – ATESTE DE RECEBIMENTO

Para fins de cumprimento do disposto no art. 33, inciso II, alínea “h”, da IN SGD/ME nº 94/2022, por este instrumento **ATESTO/ATESTAMOS** que o(s) **<serviço(s)/ bem(s)>** correspondentes à **<OS/OFB>** acima identificada foram **<prestados/entregues>** pela



CONTRATADA e ATENDEM às exigências contratuais, discriminadas abaixo, de acordo com os Critérios de Aceitação previamente definidos no Modelo de Gestão do Contrato acima indicado.

ITEM	EXIGÊNCIA CONTRATUAL	ATENDIMENTO	OBSERVAÇÃO
1	<exigência contratual estabelecida no TR >	...	
...	...	...	
...	...	...	
...	...	...	

4 – DESCONTOS EFETUADOS E VALOR A LIQUIDAR

De acordo com os critérios de aceitação e demais termos contratuais, <não> há incidência de descontos por desatendimento dos indicadores de níveis de serviços definidos.

<Não foram / Foram> identificadas inconformidades técnicas ou de negócio que ensejam indicação de glosas e sanções, <cuja instrução corre em processo administrativo próprio (nº do processo)>.

Por conseguinte, o valor a liquidar correspondente à <OS/OFB> acima identificada monta em R\$ <valor> (<valor por extenso>).

Referência: <Relatório de Fiscalização nº xxxx ou Nota Técnica nº yyyy>.

5 – ASSINATURA

GESTOR DO CONTRATO

<Nome do Gestor do Contrato>

Matrícula: xxxxxxxx

<Local>, <dia> de <mês> de <ano>.