



UNIVERSIDADE FEDERAL DO PARANÁ
Rua XV de Novembro, 1299, - Bairro Centro, Curitiba/PR, CEP 80060-000
Telefone: (41) 33605228 - <http://www.ufpr.br/>

EDITAL PREGÃO ELETRÔNICO Nº 90.002/2025

Processo nº 23075.049214/2024-91

UNIVERSIDADE FEDERAL DO PARANÁ (153079)

Objeto: Contratação de solução unificada de segurança e conectividade.

Valor Total da Contratação: R\$ 11.974.559,57

Data da Sessão Pública: Dia 28/01/2025 às 08h30min (horário de Brasília)

Data Máxima para recebimento de Impugnações e Esclarecimentos: 23/01/2025

Endereço do certame: www.gov.br/compras/pt-br/

Critério de Julgamento: Menor preço global do grupo

Modo de Disputa: Aberto

Preferência ME/EPP/EQUIPARADAS: Não

SUMÁRIO

1. Do Objeto
2. Do Registro de Preços
3. Da Participação na Licitação
4. Da Apresentação da Proposta e dos Documentos de Habilitação
5. Do Preenchimento da Proposta
6. Da Abertura da Sessão, Classificação das Propostas e Formulação de Lances
7. Da Fase de Julgamento
8. Da Fase de Habilitação
9. Da Ata de Registro de Preços
10. Da Formação do Cadastro de Reserva
11. Dos Recursos
12. Da Adjudicação e Homologação
13. Do Termo de Contrato
- 15 Das Infrações Administrativas e Sanções da Fase Licitatória
15. Da Impugnação ao Edital e do Pedido de Esclarecimento
16. Das Disposições Gerais
17. Do Foro

EDITAL DO PREGÃO ELETRÔNICO Nº 90.002/2025 - SOLUÇÃO DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO

UNIVERSIDADE FEDERAL DO PARANÁ

(Processo Administrativo nº 23075.049214/2024-91)

Torna-se público que a Universidade Federal do Paraná, autarquia federal de CNPJ 75.095.679/0001-49, por meio da Coordenadoria de Licitações e Contratações, sediada na Rua Dr. Faivre nº 105, Centro, CEP: 80.060-140 – Curitiba – Paraná, realizará licitação, para registro de preços, na modalidade PREGÃO, na forma ELETRÔNICA, nos termos da [Lei nº 14.133, de 2021](#), do Decreto nº 11.462, de 31 de março de 2023, e demais legislações aplicáveis 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 unificada de segurança e conectividade, conforme condições, quantidades e exigências estabelecidas neste Edital e seus anexos.

1.2. A licitação será realizada em grupo único, formado por 33 (trinta e três) itens, conforme tabela constante no Termo de Referência, devendo o licitante oferecer proposta para todos os itens que o compõem.

2. DO REGISTRO DE PREÇOS

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

3. DA PARTICIPAÇÃO NA LICITAÇÃO

3.1. Poderão participar deste 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).

3.1.1. Os interessados deverão atender às condições exigidas no cadastramento no Sicafe até o terceiro dia útil anterior à data prevista para recebimento das propostas.

3.2. O licitante responsabiliza-se exclusiva e formalmente pelas transações efetuadas em seu nome, assume como firmes e verdadeiras suas propostas e seus lances, inclusive os atos praticados diretamente ou por seu representante, excluindo a responsabilidade do provedor do sistema ou do órgão ou entidade promotora da licitação por eventuais danos decorrentes de uso indevido das credenciais de acesso, ainda que por terceiros.

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

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

3.5. Não serão aplicadas as disposições constantes dos arts. 42 a 49 da Lei Complementar nº 123, de 14 de dezembro de 2006, que conferem os benefícios às Microempresas e Empresas de Pequeno Porte, em atenção ao disposto do inciso I, do § 1º, do Art. 4º da Lei nº 14.133/2021, dado que o valor estimado da licitação é superior à receita bruta máxima admitida para fins de enquadramento como empresa de pequeno porte.

3.6. Não poderão disputar esta licitação:

3.6.1. Aquele que não atenda às condições deste Edital e seu(s) anexo(s);

3.6.2. Pessoa física;

3.6.3. Pessoa jurídica que se encontre, ao tempo da licitação, impossibilitada de participar da licitação em decorrência de sanção que lhe foi imposta;

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

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

3.6.6. Pessoa 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;

3.6.7. Agente público do órgão ou entidade licitante;

3.6.8. Organizações da Sociedade Civil de Interesse Público - OSCIP, atuando nessa condição;

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

3.7. O impedimento de que trata o item 3.6.3 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.

3.8. 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](#).

3.9. A vedação de que trata o item 3.6.7 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.

3.10. Antes de elaborar suas propostas, os licitantes deverão ler atentamente o Edital e demais documentos anexos, pois a participação nesta licitação significa pleno conhecimento de suas instruções, não cabendo, após sua abertura, alegação de desconhecimento de seus itens ou questionamento quanto ao seu conteúdo.

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, conforme o critério de julgamento adotado neste Edital, até a data e o horário estabelecidos para abertura da sessão pública.
- 4.3. No cadastramento da proposta inicial, o licitante declarará, em campo próprio do sistema, que:
- 4.3.1. 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;
 - 4.3.2. 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](#);
 - 4.3.3. 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](#);
 - 4.3.4. 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.
- 4.4. 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](#).
- 4.5. A falsidade da declaração de que trata o item 4.3 sujeitará o licitante às sanções previstas na [Lei nº 14.133, de 2021](#), e neste Edital.
- 4.6. 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.
- 4.7. 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.
- 4.8. 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.
- 4.9. Desde que disponibilizada a funcionalidade no sistema, o licitante poderá parametrizar o seu valor final mínimo quando do cadastramento da proposta e obedecerá às seguintes regras:
- 4.9.1. A aplicação do intervalo mínimo de diferença de valores entre os lances, que incidirá tanto em relação aos lances intermediários quanto em relação ao lance que cobrir a melhor oferta; e
 - 4.9.2. Os lances serão de envio automático pelo sistema, respeitado o valor final mínimo estabelecido e o intervalo de que trata o subitem acima.
- 4.10. O valor final mínimo parametrizado no sistema poderá ser alterado pelo fornecedor durante a fase de disputa, sendo vedado:
- 4.10.1. Valor superior a lance já registrado pelo fornecedor no sistema, quando adotado o critério de julgamento por menor preço;
- 4.11. O valor final mínimo parametrizado na forma do item 4.9 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.
- 4.12. 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.
- 4.13. 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:
- 5.1.1. Valor unitário e total do item;
 - 5.1.2. Marca e modelo (caso aplicável);
 - 5.1.2.1 Deverá ser ofertado somente uma única marca e modelo para o item cadastrado, sob pena de desclassificação.
 - 5.1.3. Fabricante (caso aplicável);
 - 5.1.4 Quantidade cotada. Devendo respeitar as quantidades descritas no termo de referência.
 - 5.1.5. Descrição do objeto, contendo as informações similares à especificação do Termo de Referência.
- 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. 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.

5.7.1. O prazo de validade da proposta não será inferior a **90 (noventa)** dias, a contar da data de sua apresentação.

5.7.2. Os licitantes devem respeitar os preços máximos estabelecidos nas normas de regência de contratações públicas federais, quando participarem de licitações públicas;

5.8. 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.

5.9. **Caso o critério de julgamento for o menor preço**, as propostas, ainda, deverão observar o seguinte:

5.9.1. Ser apresentadas com, no máximo, 02 (duas) casas após a vírgula (exemplo: R\$ 12,34), haja vista que o Sistema Monetário Nacional não contempla valores inferiores a um centavo.

5.9.2. As propostas que não atenderem ao disposto no subitem 5.9.1 acima, apresentando mais do que 02 (duas) casas decimais, quando aplicável, terão as casas excedentes desconsideradas, sendo que a Pregoeira, na fase de aceitação, registrará o novo preço no sistema, no campo "valor negociado", garantida a aceitação do valor que restar após tal procedimento.

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.

6.2.1. Será desclassificada a proposta cadastrada em campo próprio do sistema que identifique o licitante.

6.2.2. A desclassificação será sempre fundamentada e registrada no sistema, com acompanhamento em tempo real por todos os participantes.

6.2.3. A não desclassificação da proposta não impede o seu julgamento definitivo em sentido contrário, levado a efeito na fase de aceitação.

6.3. O sistema ordenará automaticamente as propostas classificadas, sendo que somente estas participarão da fase de lances.

6.4. O sistema disponibilizará campo próprio para troca de mensagens entre a Pregoeira e os licitantes.

6.5. 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.

6.6. O lance deverá ser ofertado pelo valor unitário do item.

6.7. Os licitantes poderão oferecer lances sucessivos, observando o horário fixado para abertura da sessão e as regras estabelecidas no Edital.

6.8. O licitante somente poderá oferecer lance de valor inferior ao último por ele ofertado e registrado pelo sistema.

6.9. 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 0,25% (zero virgula vinte e cinco por cento) com o valor convertido em Real.

6.10. 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.

6.11. O procedimento seguirá de acordo com o modo de disputa adotado.

6.12. O envio de lances no pregão eletrônico será pelo modo de disputa "aberto", os licitantes apresentarão lances públicos e sucessivos, com prorrogações.

6.12.1. 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.

6.12.2. 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.

6.12.3. 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.

6.12.4. Definida a melhor proposta, se a diferença em relação à proposta classificada em segundo lugar for de pelo menos 5% (cinco por cento), a Pregoeira, auxiliado pela equipe de apoio, poderá admitir o reinício da disputa aberta, para a definição das demais colocações.

6.12.5. Após o reinício previsto no item supra, os licitantes serão convocados para apresentar lances intermediários.

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 a Pregoeira, 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 a Pregoeira 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 pela Pregoeira 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. 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:

6.19.1. Caberá a aplicação das regras de preferência, sucessivamente, para:

6.19.1.1. 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;

6.19.1.2. bens e serviços com tecnologia desenvolvida no País; e

6.19.1.3. 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.

6.19.2. Os licitantes classificados que estejam enquadrados no item 6.19.1.1, 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.

6.19.3. Caso a preferência não seja exercida na forma do item 6.19.1.1, por qualquer motivo, serão convocadas as empresas classificadas que estejam enquadradas no item 6.19.1.2, na ordem de classificação, para a comprovação e o exercício do direito de preferência, aplicando-se a mesma regra para o item 6.19.1.3 caso esse direito não seja exercido.

6.20. 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.

6.20.1. 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:

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

6.20.1.2. 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 na Lei 14.133/2021;

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

6.20.1.4. Desenvolvimento pelo licitante de programa de integridade, conforme orientações dos órgãos de controle.

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

6.20.2.1. Empresas estabelecidas no território do Estado do Paraná;

6.20.2.2. Empresas brasileiras;

6.20.2.3. Empresas que invistam em pesquisa e no desenvolvimento de tecnologia no País;

6.20.2.4. Empresas que comprovem a prática de mitigação, nos termos da [Lei nº 12.187, de 29 de dezembro de 2009](#).

6.21. Encerrada a etapa de envio de lances da sessão pública, na hipótese da proposta do primeiro colocado permanecer acima do preço máximo definido para a contratação, a Pregoeira poderá negociar condições mais vantajosas, após definido o resultado do julgamento.

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

6.21.2. A negociação será realizada por meio do sistema, podendo ser acompanhada pelos demais licitantes.

6.21.3. O resultado da negociação será divulgado a todos os licitantes e anexado aos autos do processo licitatório.

6.21.4. Em todo caso a Administração não contratará valor(s) acima do máximo estabelecido no Termo de Referência deste Edital.

6.21.5. A Pregoeira solicitará ao licitante mais bem classificado que, no prazo mínimo de 2 (duas) horas, envie a proposta adequada ao último lance ofertado após a negociação realizada, acompanhada, se for o caso, dos documentos complementares, quando necessários à confirmação daqueles exigidos neste Edital e já apresentados.

6.21.6. É facultado à Pregoeira prorrogar o prazo estabelecido, a partir de solicitação fundamentada feita no chat pelo licitante, antes de findo o prazo.

6.22. Após a negociação do preço, a Pregoeira iniciará a fase de aceitação e julgamento da proposta.

7. DA FASE DE JULGAMENTO

7.1. Encerrada a etapa de negociação, a Pregoeira 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 3.6 do edital, especialmente quanto à existência de sanção que impeça a participação no certame ou a futura contratação, mediante a consulta aos seguintes cadastros:

a) SICAF;

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

c) 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, a Pregoeira 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. Será desclassificada a proposta vencedora que:

7.5.1. Contiver vícios insanáveis;

7.5.2. Não obedecer às especificações técnicas contidas no Termo de Referência;

7.5.3. Apresentar preços inexequíveis ou permanecerem acima do preço máximo definido para a contratação;

7.5.4. Não tiverem sua exequibilidade demonstrada, quando exigido pela Administração;

7.5.5. Apresentar desconformidade com quaisquer outras exigências deste Edital ou seus anexos, desde que insanável.

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

7.6.1. A inexequibilidade, na hipótese de que trata o **caput**, só será considerada após diligência da Pregoeira, que comprove:

7.6.1.1. Que o custo do licitante ultrapassa o valor da proposta; e

7.6.1.2. Inexistirem custos de oportunidade capazes de justificar o vulto da oferta.

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

7.8. 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.

8.2. 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.

8.2.1. 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 20% para o consórcio em relação ao valor exigido para os licitantes individuais.

8.3. Os documentos exigidos para fins de habilitação deverão ser enviados no formato digital através do Sistema de Compras do Governo.

8.4. 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.

8.5. 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](#)).

8.6. 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.

8.7. 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.

8.8. A habilitação será verificada por meio do Sicafe, nos documentos por ele abrangidos.

8.8.1. 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](#)).

8.9. É de responsabilidade do licitante conferir a exatidão dos seus dados cadastrais no Sicafe 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](#)).

8.9.1. A não observância do disposto no item anterior poderá ensejar desclassificação no momento da habilitação. ([IN nº 3/2018, art. 7º, parágrafo único](#)).

8.10. A verificação pela Pregoeira, em sítios eletrônicos oficiais de órgãos e entidades emissores de certidões constitui meio legal de prova, para fins de habilitação.

8.10.1. Os documentos exigidos para habilitação que não estejam contemplados no Sicafe serão enviados por meio do sistema, em formato digital, no prazo de no mínimo 02 (duas) horas, prorrogável por igual período, contado da solicitação da Pregoeira, sob pena de desclassificação.

8.11. A verificação no Sicafe ou a exigência dos documentos nele não contidos somente será feita em relação ao licitante vencedor.

8.11.1. 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.

8.12. 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](#)):

8.12.1. 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

8.12.2. Atualização de documentos cuja validade tenha expirado após a data de recebimento das propostas;

8.13. 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.

8.14. Na hipótese de o licitante não atender às exigências para habilitação, a Pregoeira 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 8.10.1.

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

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.

9.2. 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:

- a) A solicitação seja devidamente justificada e apresentada dentro do prazo; e
- b) 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:

- a) dos licitantes que aceitarem cotar o objeto com preço igual ao do adjudicatário, observada a classificação na licitação; e
- b) 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:

- a) quando o licitante vencedor não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital; ou
- b) 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:

- a) 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
- b) 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:

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 fraqueada aos interessados no endereço [:: Sistema Eletrônico de Informações - Pesquisa Pública :: \(ufpr.br\)](https://sei.ufpr.br), mediante informação do número do processo administrativo.

Sistema Eletrônico de Informações - Pesquisa Pública (ufpr.br): Endereço eletrônico

[https://sei.ufpr.br/sei/web/modulos/pesquisa/md_pesq_processo_pesquisar.php?](https://sei.ufpr.br/sei/web/modulos/pesquisa/md_pesq_processo_pesquisar.php?acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0)

[acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0.](https://sei.ufpr.br/sei/web/modulos/pesquisa/md_pesq_processo_pesquisar.php?acao_externa=protocolo_pesquisar&acao_origem_externa=protocolo_pesquisar&id_orgao_acesso_externo=0)

12. DA ADJUDICAÇÃO E HOMOLOGAÇÃO

12.1. O objeto da licitação será adjudicado ao licitante declarado vencedor, por ato da autoridade competente, após a regular decisão dos eventuais recursos apresentados.

12.2. Após a fase recursal, constatada a regularidade dos atos praticados, a autoridade competente homologará o procedimento licitatório.

13. DO TERMO DE CONTRATO

13.1. Após a homologação da licitação, em sendo realizada a contratação, será firmado Contrato.

13.1.1. Para os itens relativos a Serviços de configuração (2, 4, 6, 13, 16, 18, 20, 22, 25, 27, 29) o instrumento de contrato será substituído pela nota de empenho.

13.1.2. Para os demais itens deverá ser firmado contrato de acordo com os prazos de vigência descritos nos itens 1.8 a 1.10 do Termo de Referência (Anexo I deste Edital).

13.2. A contratação da empresa, respeitados os demais critérios aqui descritos, far-se-á através da assinatura do contrato (Anexo IV deste Edital), nas condições estabelecidas neste Edital.

13.2.1. Recomenda-se que os licitantes providenciem seu cadastro no sistema de processo eletrônico da UFPR, visando agilizar os trâmites para assinatura do contrato (Anexo IV deste Edital).

13.2.1.1. O cadastro deve ser feito pelo representante legal da empresa, no sítio sei.ufpr.br escolhendo a opção "Você é ALUNO ou usuário externo? Clique AQUI para acessar o SEI." no alto da página.

13.2.1.2. A assinatura do contrato (Anexo IV deste Edital) poderá ser realizada através do Sistema de Processo Eletrônico da UFPR.

13.2.1.2.1. Não haverá envio de documentos por correio nas situações cuja assinatura do contrato (Anexo IV deste Edital) seja realizada através do Sistema de Processo Eletrônico da UFPR.

13.3. O licitante vencedor terá o prazo de 05 (cinco) dias úteis, contados a partir da data de sua convocação, para assinar o Contrato (Anexo IV deste Edital), sob pena de decair do direito à contratação, sem prejuízo das sanções previstas neste Edital.

13.3.1. O prazo previsto no subitem anterior poderá ser prorrogado, por igual período, por solicitação justificada do licitante vencedor e aceita pela Administração.

13.3.2. Caso a proponente não tenha providenciado seu cadastro no sistema de processo eletrônico da UFPR (SEI), conforme disposto no item 13.2.1 acima, o mesmo se fará obrigatório antes da assinatura do contrato (Anexo IV deste Edital), caso a assinatura ocorra no referido sistema.

13.3.3. Caso a assinatura não seja realizada através do sistema de processo eletrônico da UFPR, o contrato será enviado por e-mail, para o endereço informado na proposta pelo licitante, e deverá ser devolvido, assinado em duas vias, por correio, para a Unidade de Contratos da Coordenadoria de Licitações e Contratações da UFPR.

13.3.3.1. Recebidas as vias do Contrato assinadas pelo licitante, estas serão assinadas pela autoridade competente da UFPR e disponibilizadas no endereço eletrônico da Coordenadoria de Licitações e Contratações da UFPR (<https://pra.ufpr.br/licitacoes/gerencia-de-contratos/>), e o extrato do contrato será publicado no Diário Oficial da União.

13.4. A assinatura do contrato (Anexo IV deste Edital) implica no reconhecimento de que:

a) A contratada se vincula à sua proposta e às previsões contidas no edital e seus anexos;

b) A contratada reconhece que as hipóteses de extinção do contrato são aquelas previstas nos artigos 137 da Lei nº 14.133/2021 e reconhece os direitos da Administração previstos nos artigos 138 e 139 da mesma Lei.

13.5. Previamente à contratação a Administração realizará consulta ao SICAF para identificar possível suspensão temporária de participação em licitação, no âmbito do órgão ou entidade, proibição de contratar com o Poder Público, bem como ocorrências impeditivas indiretas, observado o disposto no art. 29, da Instrução Normativa nº 3, de 26 de abril de 2018, e nos termos do art. 6º, III, da Lei nº 10.522, de 19 de julho de 2002, consulta prévia ao CADIN.

13.6. Para comprovação de poderes para a assinatura do contrato, deverão ser apresentados os seguintes documentos:

a) Se for sócio, fotocópia autenticada do contrato social, da última alteração contratual e da Certidão Simplificada da Junta emitida há menos de 30 (trinta) dias da data de abertura da licitação;

b) Se for procurador, fotocópia autenticada do instrumento de procuração, do contrato social, da última alteração contratual e da Certidão Simplificada da Junta Comercial emitida há menos de 30 (trinta) dias da data de abertura da licitação;

c) As procurações deverão demonstrar de maneira expressa que o outorgado recebeu poderes para firmar propostas e assinar contratos;

d) Os contratos sociais deverão comprovar que o outorgante tem poderes para substabelecimento;

e) As Certidões Simplificadas da Junta Comercial deverão comprovar que a última alteração contratual arquivada é a mesma que está sendo apresentada na licitação.

13.7. Na assinatura do contrato será exigida a comprovação das condições de habilitação consignadas no edital, que deverão ser mantidas pelo licitante durante a vigência do contrato.

13.8. Na hipótese de o vencedor da licitação não comprovar as condições de habilitação consignadas no edital ou se recusar a assinar o contrato, a Administração, sem prejuízo da aplicação das sanções das demais cominações legais cabíveis a esse licitante, poderá convocar outro licitante, respeitada a ordem de classificação, para, após a comprovação dos requisitos para habilitação, analisada a proposta e eventuais documentos complementares e, feita a negociação, assinar o contrato.

13.9. Para efeito de emissão de nota fiscal/fatura, será utilizado o Cadastro Nacional de Pessoa Jurídica - CNPJ, referente àquele que a licitante participou do certame, não sendo possível, assim, faturar com CNPJ distinto.

14. DAS INFRAÇÕES ADMINISTRATIVAS E SANÇÕES DA FASE LICITATÓRIA

14.1. Comete infração administrativa, nos termos da lei, o licitante que, com dolo ou culpa:

14.1.1. Deixar de entregar a documentação exigida para o certame ou não entregar qualquer documento que tenha sido solicitado pela Pregoeira durante o certame;

14.1.2. Salvo em decorrência de fato superveniente devidamente justificado, não mantiver a proposta, em especial, quando:

14.1.2.1. Não enviar a proposta adequada ao último lance ofertado ou após a negociação;

14.1.2.2. Recusar-se a enviar o detalhamento da proposta quando exigível;

14.1.2.3. Pedir para ser desclassificado quando encerrada a etapa competitiva; ou

14.1.3. Não celebrar a Ata de Registro de Preços/Contrato ou não entregar a documentação exigida para a contratação, quando convocado dentro do prazo de validade de sua proposta;

14.1.3.1. 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;

14.1.4. Apresentar declaração ou documentação falsa exigida para o certame ou prestar declaração falsa durante a licitação.

14.1.5. Fraudar a licitação.

14.1.6. Comportar-se de modo inidôneo ou cometer fraude de qualquer natureza, em especial quando:

14.1.6.1. Agir em conluio ou em desconformidade com a lei;

14.1.6.2. Induzir deliberadamente a erro no julgamento;

14.1.7. Praticar atos ilícitos com vistas a frustrar os objetivos da licitação

14.1.8. Praticar ato lesivo previsto no [art. 5º da Lei n.º 12.846, de 2013](#).

14.2. 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:

14.2.1. Advertência;

14.2.2. Multa;

14.2.3. Impedimento de licitar e contratar e

14.2.4. 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.

14.3. Na aplicação das sanções serão considerados:

14.3.1. A natureza e a gravidade da infração cometida.

14.3.2. As peculiaridades do caso concreto

14.3.3. As circunstâncias agravantes ou atenuantes

14.3.4. O danos que dela provierem para a Administração Pública

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

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

14.4.1 Para as infrações previstas nos itens 14.1.1, 14.1.2 e 14.1.3, a multa será de 0,5% a 15% do valor do contrato lícitado.

14.4.2 Para as infrações previstas nos itens 14.1.4, 14.1.5, 14.1.6, 14.1.7 e 14.1.8, a multa será de 15% a 30% do valor do contrato lícitado.

14.4.3. A partir do trânsito em julgado da decisão administrativa de imposição de multa administrativa, os valores devidos estarão sujeitos a atualização monetária, incidindo a taxa referencial do Sistema Especial de Liquidação e de Custódia (SELIC) acumulada mensalmente, calculada a partir do mês subsequente ao da consolidação até o mês anterior ao do pagamento, e 1% (um por cento) relativamente ao mês em que o pagamento estiver sendo efetuado (previsão da [Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022](#)).

14.5. 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.

14.5.1 Os parâmetros de aplicação das sanções administrativas no âmbito da UFPR serão os seguintes:

Falha apurada	Fundamento legal	Sanção	Multa
Deixar de entregar a documentação exigida para o certame	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 30 dias	Até 5% em relação ao valor de sua proposta
Não entregar documento solicitado durante o certame	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 15 dias	Até 3% em relação ao valor de sua proposta
Deixar de manter as condições de habilitação, durante a realização do certame	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 60 dias	Até 10% em relação ao valor de sua proposta
Recusar-se ou deixar de responder diligência realizada pela UFPR, durante a análise da proposta ou da planilha de custos da licitação	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 60 dias	Até 10% em relação ao valor de sua proposta
Não enviar proposta adequada ao último lance ofertado ou após a negociação	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 60 dias	Até 10% em relação ao valor de sua proposta
Recusar-se a enviar o detalhamento da proposta	Lei 14.133/2021, art. 155 inc. IV	Impedimento de licitar e contratar no âmbito da União por até 60 dias	Até 10% em relação ao valor de sua proposta
Pedir para ser desclassificado quando encerrada a etapa competitiva	Lei 14.133/2021, art. 155 inc. V	Impedimento de licitar e contratar no âmbito da União por até 30 dias	Até 5% em relação ao valor de sua proposta
Não celebrar o contrato ou ata de registro de preços	Lei 14.133/2021, art. 155 inc. VI	Impedimento de licitar e contratar no âmbito da União por até 6 meses	Até 15% em relação ao valor de sua proposta
Não entregar a documentação exigida para a contratação	Lei 14.133/2021, art. 155 inc. VI	Impedimento de licitar e contratar no âmbito da União por até 6 meses	Até 15% em relação ao valor de sua proposta
Não se cadastrar no sistema de processo eletrônico da UFPR para assinatura da Ata ou Contrato	Lei 14.133/2021, art. 155 inc. VI	Impedimento de licitar e contratar no âmbito da União por até 6 meses	Até 15% em relação ao valor de sua proposta
Apresentar declaração ou documentação falsa exigida para o certame	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 48 meses	Até 20% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Prestar declaração falsa durante a licitação	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 48 meses	Até 20% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Fraudar a licitação	Lei 14.133/2021, art. 155 inc. IX	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 48 a 60 meses	Até 30% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Agir em conluio ou em desconformidade com a lei	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 48 a 60 meses	Até 30% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Induzir deliberadamente a erro no julgamento	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 48 meses	Até 20% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Omitir informações em quaisquer documentos exigidos no certame licitatório	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 48 meses	Até 20% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Adulterar documento, público ou particular, com o fim de prejudicar direito, criar obrigação ou alterar a verdade:	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 48 meses	Até 20% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Praticar atos ilícitos com vistas a frustrar os objetivos da licitação	Lei 14.133/2021, art. 155 inc. XI	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
Participação na licitação de empresa constituída com a finalidade de burlar penalidade aplicada anteriormente	Lei 14.133/2021, art. 155 inc. XI	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.

Praticar ato lesivo previsto no art. 5º da Lei n.º 12.846, de 2013	Lei 14.133/2021, art. 155 inc. XII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% em relação ao valor total homologado na licitação. Caso o certame tenha sido frustrado, a base de cálculo da multa será o valor estimado para a licitação.
--	------------------------------------	---	--

14.5.1.1 As sanções listadas na tabela acima não esgotam a possibilidade de enquadramento das condutas do licitante nas infrações previstas nesta Seção, com a aplicação das penalidades cabíveis.

14.6. 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.

14.7. A sanção de impedimento de licitar e contratar será aplicada ao responsável em decorrência das infrações administrativas relacionadas nos itens 14.1.1, 14.1.2 e 14.1.3, quando não se justificar a imposição de penalidade mais grave, e impedirá o responsável de licitar e contratar com a União, pelo prazo máximo de 3 (três) anos.

14.8. Poderá ser aplicada ao responsável a sanção de declaração de inidoneidade para licitar ou contratar com toda a Administração Pública, em decorrência da prática das infrações dispostas nos itens 14.1.4, 14.1.5, 14.1.6, 14.1.7 e 14.1.8, bem como pelas infrações administrativas previstas nos itens 14.1.1, 14.1.2 e 14.1.3 que justifiquem a imposição de penalidade mais grave que a sanção de impedimento de licitar e contratar com a União, cuja duração observará o prazo previsto no [art. 156, §5º, da Lei n.º 14.133/2021](#).

14.9. 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 14.1.3, 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.

14.10. 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.

14.11. 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.

14.12. 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.

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

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

15. DA IMPUGNAÇÃO AO EDITAL E DO PEDIDO DE ESCLARECIMENTO

15.1. 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.

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

15.3. A impugnação e o pedido de esclarecimento poderão ser realizados por forma eletrônica, para o e-mail: licita@ufpr.br.

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

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

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

16. DAS DISPOSIÇÕES GERAIS

16.1. Será divulgada ata da sessão pública no sistema eletrônico.

16.2. 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.

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

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

16.5. 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.

16.6. 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.

16.7. 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.

16.8. 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.

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

16.10. O Edital e seus anexos estão disponíveis, na íntegra, no Portal Nacional de Contratações Públicas (PNCP) e endereço eletrônico <https://pra.ufpr.br/licitacoes/>.

16.11. A entrega da proposta implica na automática aceitação pela proponente, sem nenhuma ressalva, de todas as condições estabelecidas neste Edital e seus anexos.

17. DO FORO

17.1. Por força do disposto no artigo 109, inciso I da Constituição Federal, o foro da Justiça Federal - Seção Judiciária do Paraná / Subseção Judiciária de Curitiba será competente para resolver questões relativas ao presente instrumento, bem como para as atas de registros de preços dele decorrentes, conforme [art. 92, §1º, da Lei nº 14.133/21](#).

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

ANEXO I - Termo de Referência

- Anexo A - Especificações Técnicas dos Itens
- Anexo B - Endereços da UFPR no Paraná
- Anexo C - Termo de Compromisso e Manutenção de Sigilo
- Anexo D - Termo de Ciência
- Anexo E - Declaração de Inexistência de Registro de Oportunidade
- Anexo F - Declaração de Garantia
- Anexo G - Modelo de Proposta

ANEXO II - Estudo Técnico Preliminar

ANEXO III - Minuta de Ata de Registro de Preços

ANEXO IV - Minuta de Termo de Contrato

SANDRA MARA REIS DOS SANTOS
Pregoeira Oficial
Portaria/PRA Nº 026/2024

Curitiba, 13 de janeiro de 2025.



Documento assinado eletronicamente por SANDRA MARA REIS DOS SANTOS, ASSESSOR(A) DA UNIDADE DE PLANEJAMENTO E CONTROLE - CLIC/PRA, em 13/01/2025, às 14:00, conforme art. 1º, III, "b", da Lei 11.419/2006.



A autenticidade do documento pode ser conferida [aqui](#) informando o código verificador 7418381 e o código CRC 697A3DFA.

ANEXO I
TERMO DE REFERÊNCIA COMPRA DE TIC - LEI 14.133/2021

Processo nº 23075.049214/2024-91

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

1. CONDIÇÕES GERAIS DA CONTRATAÇÃO

1.1. Contratação de solução unificada de segurança e conectividade, nos termos da tabela abaixo, conforme condições e exigências estabelecidas neste instrumento.

Tabela 1 - Itens da solução a ser contratada

LOTE	ITEM	ESPECIFICAÇÃO	CATMAT / CATSER	Métrica	Qtde	Valor Unitário	Valor Total
------	------	---------------	-----------------	---------	------	----------------	-------------

1	SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses	609340	Unidade	2	R\$ 1.208.599,62	R\$ 2.417.199,24
2	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO I	27014	Unidade	2	R\$ 25.397,93	R\$ 50.795,86
3	SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses	609340	Unidade	2	R\$ 495.832,22	R\$ 991.664,44
4	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO II	27014	Unidade	2	R\$ 21.806,22	R\$ 43.612,44
5	SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses	609340	Unidade	2	R\$ 58.015,89	R\$ 116.031,78
6	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO III	27014	Unidade	2	R\$ 15.364,51	R\$ 30.729,02
7	PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses	393277	Unidade	1.100	R\$ 4.237,05	R\$ 4.660.755,00
8	PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses	393277	Unidade	100	R\$ 6.973,19	R\$ 697.319,00
9	PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses	393277	Unidade	20	R\$ 9.983,53	R\$ 199.670,60
10	INJETOR PoE (Power Injector)	426731	Unidade	50	R\$ 1.618,24	R\$ 80.912,00
11	SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	27464	Unidade	1	R\$ 26.948,01	R\$ 26.948,01
12	LICENÇAS PARA SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO) PARA 1.000 DISPOSITIVOS	27502	Unidade	5	R\$ 99.772,61	R\$ 498.863,05
13	SERVIÇO DE CONFIGURAÇÃO PARA LICENÇA DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	27014	Unidade	1	R\$ 23.743,97	R\$ 23.743,97

1	14	SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO	27464	Unidade	1	R\$ 10.633,50	R\$ 10.633,50
	15	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I (1.000 DISPOSITIVOS)	27502	Unidade	5	R\$ 30.662,53	R\$ 153.312,65
	16	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I	27014	Unidade	1	R\$ 23.743,97	R\$ 23.743,97
	17	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II (10.000 DISPOSITIVOS)	27502	Unidade	1	R\$ 183.229,63	R\$ 183.229,63
	18	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II	27014	Unidade	1	R\$ 37.368,35	R\$ 37.368,35
	19	SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	27502	Unidade	1	R\$ 132.323,72	R\$ 132.323,72
	20	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	27014	Unidade	1	R\$ 28.285,43	R\$ 28.285,43
	21	SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	27502	Unidade	2	R\$ 67.111,62	R\$ 134.223,24
	22	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	27014	Unidade	1	R\$ 32.826,89	R\$ 32.826,89
	23	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO I (25GB/DIA)	27502	Unidade	2	R\$ 67.663,38	R\$ 135.326,76
	24	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO II (500GB/DIA)	27502	Unidade	1	R\$ 448.132,21	R\$ 448.132,21
	25	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS	27014	Unidade	1	R\$ 19.202,51	R\$ 19.202,51
	26	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL (ATÉ 10 FIREWALLS)	27502	Unidade	1	R\$ 5.778,74	R\$ 5.778,74
	27	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL	27014	Unidade	1	R\$ 23.743,97	R\$ 23.743,97

28	SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES (LICENÇA DE 3 ANOS PARA 2.000 USUÁRIOS)	27502	Unidade	3	R\$ 147.103,24	R\$ 441.309,72
29	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES	27014	Unidade	3	R\$ 30.682,55	R\$ 92.047,65
30	TRANSCEIVER 10GE SFP+ SR: Multimodo, LC Duplex, 300m	462024	Unidade	24	R\$ 846,09	R\$ 20.306,16
31	TRANSCEIVER 10GE SFP+ LR: Monomodo, LC Duplex, 10km	462023	Unidade	12	R\$ 1.699,84	R\$ 20.398,08
32	TRANSCEIVER 40GE QSFP+ SR: Multimodo, MPO, 150m	618355	Unidade	16	R\$ 4.598,12	R\$ 73.569,92
33	TRANSCEIVER 40GE QSFP+ LR: Monomodo, LC Duplex, 10km	618355	Unidade	6	R\$ 20.092,01	R\$ 120.552,06
Valor Estimado:						R\$ 11.974.559,57

1.2. Os bens objetos desta contratação são caracterizados como comuns, uma vez que seus padrões de desempenho e qualidade possam ser objetivamente definidos pelo edital, por meio de especificações usuais no mercado.

1.3. O objeto desta contratação não se enquadra como sendo bem de luxo, conforme Decreto nº 10.818, de 27 de setembro de 2021.

1.4. Os serviços a serem contratados enquadram-se nos pressupostos do Decreto nº 9.507 de 2018, constituindo-se em atividades materiais acessórias, instrumentais ou complementares à área de competência legal da UFPR, não inerentes às categorias funcionais abrangidas por seu respectivo plano de cargos.

1.5. A prestação dos serviços não gera vínculo empregatício entre os empregados da CONTRATADA e a Administração CONTRATANTE, vedando-se qualquer relação entre estes que caracterize pessoalidade e subordinação direta.

1.6. O prazo de vigência da Ata de Registro de Preços será de 12 meses contados da assinatura da Ata de Registro de Preços, na forma do artigo 84 da Lei nº 14.133, de 2021, podendo o saldo remanescente ser prorrogado por até 12 meses.

1.7. **Para os itens relativos a Serviços de configuração (itens 2, 4, 6, 13, 16, 18, 20, 22, 25, 27, 29) o instrumento de contrato será substituído pela nota de empenho**, em atenção à disposição do art. 95 da Lei nº 14.133/2021.

1.8. **Para a aquisição de equipamentos (itens 1, 3, 5, 30, 31, 32 e 33)**, deverá ser firmado contrato com prazo de vigência de 60 (sessenta) meses, contados da

nrato, visando garantir os requisitos de manutenção previstos no título 4.4 deste Termo de Referência, na forma do artigo 106 da Lei nº 14.1333, de 2021.

1.9. **Para a aquisição de equipamentos (itens 7, 8, 9 e 10)**, deverá ser firmado contrato com prazo de vigência de 36 (trinta e seis) meses, contados da assinatura do contrato, visando garantir os requisitos de manutenção previstos no título 4.4 deste Termo de Referência, na forma do artigo 106 da Lei nº 14.1333, de 2021.

1.10. **Para a solução de softwares e licenças (itens 11, 12, 14, 15, 17, 19, 21, 23, 24, 26 e 28)**, deverá ser firmado contrato com vigência de 36 (trinta e seis) meses), prorrogáveis por até 120 (cento e vinte) meses, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, visando garantir os requisitos de manutenção previstos no título 4.4 deste Termo de Referência e a renovação das licenças adquiridas.

1.11. Anexos do Termo de Referência

1.11.1. Compõem este Termo de Referência os seguintes anexos:

- Anexo A – ESPECIFICAÇÕES TÉCNICAS DOS ITENS;
- Anexo B – ENDEREÇOS DA UFPR NO PARANÁ;
- Anexo C – TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO;
- Anexo D – TERMO DE CIÊNCIA;
- Anexo E – DECLARAÇÃO DE INEXISTÊNCIA DE REGISTRO DE OPORTUNIDADE;

f) Anexo F – DECLARAÇÃO DE GARANTIA.

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

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

2.2. A solução de TIC consiste em equipamentos, softwares e serviços para implementar segurança e conectividade e tem por objetivo atender as medidas previstas no Programa de Privacidade e Segurança da Informação (PPSI), permitindo à UFPR resguardar seus dados e sistemas críticos contra ameaças cibernéticas, enquanto atualiza sua infraestrutura de TIC para sustentar o crescimento e as exigências futuras.

2.3. Detalhamento das Especificações Técnicas dos Bens/Serviços

2.3.1. As especificações técnicas para cada um dos itens do pregão estão descritas no Anexo A - ESPECIFICAÇÕES TÉCNICAS DOS ITENS.

3. FUNDAMENTAÇÃO E DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

3.1. Contextualização e Justificativa da Contratação

3.1.1. A Universidade Federal do Paraná (UFPR) é uma instituição de ensino e pesquisa, cuja infraestrutura de Tecnologia da Informação e Comunicação (TIC) desempenha papel essencial no suporte às suas atividades acadêmicas, administrativas e científicas. Em 2019, a UFPR implementou importantes medidas para proteger seus ativos digitais, incluindo uma solução de firewall composta por 2 equipamentos Fortinet 3200D e conjunto de funcionalidades.

3.1.2. Contudo, a rápida evolução tecnológica e o crescimento das demandas institucionais impõem desafios significativos, especialmente no que tange à segurança da informação e à capacidade de expansão da rede. Adicionalmente, a falta de cobertura de suporte técnico, atualizações e garantia para os equipamentos de segurança de rede agrava o cenário, fragilizando a infraestrutura da universidade com a perda de funcionalidades essenciais.

3.1.3. O recente diagnóstico da UFPR sobre os controles de segurança da informação, à luz das exigências estabelecidas no Programa de Privacidade e Segurança da Informação (PPSI) e Política de Segurança da Informação e Comunicação na UFPR (POSIC), revelou lacunas que precisam ser endereçadas para mitigar riscos de segurança cibernética. Entre os principais problemas estão a ausência de inventário e controle de ativos atualizados, além de deficiências em controles de acesso e autenticação.

3.1.4. Outro aspecto crucial é a conectividade e segurança da rede sem fio da UFPR. Nos últimos anos, cada usuário passou a utilizar entre um e três dispositivos móveis, resultando em um aumento exponencial no número de dispositivos conectados. Esse crescimento intensificou a carga sobre os pontos de acesso existentes, sobrecarregando a capacidade da infraestrutura atual e ocasionando lentidão na navegação e indisponibilidade.

3.1.5. Para garantir a continuidade e qualidade dos serviços é imprescindível atualizar e expandir a infraestrutura da rede sem fio da UFPR. Isso inclui a aquisição de novos equipamentos, modernização de software e hardware, e a implementação de estratégias que atendam às necessidades presentes e futuras da comunidade universitária (levantamentos realizados indicam a necessidade de aproximadamente 1.218 novos pontos de acesso).

3.1.6. Diante desse quadro, a UFPR precisa de uma solução abrangente que atenda tanto as lacunas de segurança quanto as exigências de conectividade, alinhando-se às recomendações do PPSI e à necessidade de garantir a segurança e a integridade de seus dados e serviços.

3.1.7. A justificativa para a adoção do Sistema de Registro de Preços na presente contratação se baseia nos Incisos I, II e V, do Art. 3º, do Decreto n.º 11.462/2023.

3.2. Da Adesão à Ata de Registro de Preços

3.2.1. Será permitida a adesão de órgãos não participantes durante a vigência da Ata de Registro de Preços, desde que autorizada por essa unidade gestora e aceita pelo fornecedor, nos termos dos artigos 31 e 32 do Decreto nº 11.462/2023. Justificamos ainda que esta permissão, torna o pregão mais atrativo aos licitantes, de forma que exista maior competitividade, melhores preços, proporcionando economia para a UFPR. Ademais, os itens licitados são objetos comuns a várias instituições de ensino e outros órgãos que necessitem aprimorar seus ambientes em termos de segurança da informação e conectividade.

3.3. Justificativa Técnica da Escolha da Solução

3.3.1. Do ponto de vista técnico, a aquisição de equipamentos e softwares com as garantias especificadas assegura o atendimento pleno dos requisitos técnicos necessários para melhor aproveitamento da solução.

3.3.2. Destaque-se os seguintes aspectos técnicos:

- Aproveitamento do conhecimento técnico já adquirido na gestão da solução de Next Generation Firewall do fabricante Fortinet, uma vez que os demais componentes agregados na presente contratação utilizam a mesma (lógica de) interface de gerenciamento.
- A análise centralizada de logs de auditoria de todos os componentes da solução, permitindo a identificação mais eficiente e efetiva da ameaça.
- A adição de camada de segurança na gestão de vulnerabilidades providas da rede wi-fi, a qual possui a maior superfície de ataque na UFPR, dada sua abrangência.
- O ganho de performance, da capacidade e o aumento da cobertura da rede wi-fi somente possíveis com a ampliação e modernização do parque de access points.
- O fato de que a solução de antenas (access points) do fabricante Fortinet não necessitam de licenças para operar.
- O maior controle das redes, que poderão filtrar e controlar quais dispositivos ou usuários se conectam à rede, permitindo que sejam automaticamente direcionados para a rede apropriada (segmentação de rede) baseado em políticas de segurança.
- O suporte controlado por ferramentas especializadas no permissionamento de usuários com privilégios elevados.
- A adição de uma camada extra, avançada e em tempo real no controle de phishing e outros malwares na solução de e-mail do Microsoft 365, sobretudo capazes de reduzir a invasão de contas de usuários, um problema recorrente e de difícil gestão sem ferramentas apropriadas.
- O adequado nível de controle de acesso ao prover identificação e autenticação de visitantes nas redes internas, hoje não disponíveis de maneira segura (as redes para eventos são disponibilizadas com senha única e não se conhece a identidade do ingressante).

3.4. Justificativa Econômica da Escolha da Solução

3.4.1. Do ponto de vista econômico, foram avaliadas as soluções disponíveis no mercado e em outros órgãos e após análise das soluções, suas vantagens, desvantagens e custos totais de propriedade, a escolha da solução a ser contratada é justificada por apresentar os aspectos que visam garantir maior eficácia, eficiência, efetividade e economicidade à contratação.

3.5. Alinhamento ao Plano de Contratações Anual

3.5.1. O objeto da contratação está previsto no Plano de Contratações Anual 2024, conforme consta das informações básicas deste Termo de Referência:

I) ID PCA no PNCP: 75095679000149-0-000001/2024

II) Data de publicação no PNCP: 19/05/2023

III) Id do item no PCA: Não informado (lançamento extemporâneo).

IV) Classe/Grupo:

- Classe 7050 - Equipamentos De Rede De Tic - Local E Remota.
- Grupo 166 - Serviços de Manutenção e Instalação de Equipamentos de TIC.

V) Identificador da Futura Contratação: 153079-443/2024

VI) Nome da Futura Contratação: Aquisição de solução unificada de segurança e conectividade.

3.6. Alinhamento aos Instrumentos de Planejamento Institucionais

3.6.1. O objeto da contratação também está alinhado com a Estratégia Federal de Governo Digital (EFGD) 2024-2027 e em consonância com o Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC) 2022-2026 da Universidade Federal do Paraná, conforme demonstrado na Tabela 2:

Tabela 2 – Alinhamento ao PDTIC 2022-2026:

ID	Objetivo Estratégico	
OE.01	Posicionar a TIC como parceira estratégica da UFPR, contribuindo ativamente para o atingimento dos objetivos institucionais.	
OE.02	Prover infraestrutura e demais recursos de TIC necessários, adequados às atividades finalísticas.	
OE.03	Garantir melhoria contínua da qualidade da prestação de serviços de TIC.	
OE.04	Garantir a segurança da informação e comunicação, a privacidade de informações sigilosas e demais aspectos da segurança institucional.	
OE.05	Aprimorar a Gestão e fortalecer a Governança Digital.	
OE.07	Aprimorar o atendimento e conquistar altos índices de satisfação dos usuários e clientes de serviços digitais.	
OE.16	Promover a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).	
OE.17	Aumentar o iGovTI (Índice de Governança e Gestão de TI) e o iGestTI (Índice de Capacidade em Gestão de TI) a fim de contribuir para o aumento do IGG (índice Integrado de Governança e Gestão) estipulados pelo TCU.	
ID	Necessidade	Descrição da necessidade
NE.02	Manter a Infraestrutura de redes de dados.	Mapear, manter, suportar, prover atualização tecnológica e atender demandas por ampliação de toda a infraestrutura de rede de dados (metálica e ótica) da UFPR, incluindo ativos de rede, nobreaks e racks, etc., propiciando conectividade com disponibilidade.
NE.03	Manter, ampliar e melhorar a conectividade da rede sem fio corporativa (UFPR sem Fio).	Manter a rede sem fio da UFPR funcional, provendo suporte, renovação, ampliação, melhorias e ajustes nos serviços que garantam a disponibilidade e a conectividade para o acesso, facilidade de uso, segurança e a qualidade do serviço.
NE.12	Prover a segurança das informações e comunicações institucionais.	Prover os recursos e as soluções tecnológicas necessárias para implementar e manter a Política de Segurança da Informação (PSI) da UFPR.
NE.14	Reestruturar e manter ambientes de TIC em laboratórios e salas.	Prover suporte na estruturação e reestruturação de laboratórios de informática, assim como em salas de aula, relativamente a recursos de TIC.
NE.19	Implementar a Política de Segurança da Informação da UFPR pela TIC.	Implementar as determinações da PSI, provendo os recursos necessários, conforme Resolução nº 21/14-COPLAD, de 24/09/2014, que cria a Política de Segurança da Informação da UFPR (PSI/UFPR).
NP.03	Readequar e ampliar a rede sem fio corporativa (UFPR sem fio).	Readequar a rede sem fio da UFPR, promovendo constante atualização tecnológica, ampliação de cobertura conforme necessidade, inclusive para salas de aula, e provendo melhorias no atual serviço que garantam a disponibilidade e a conectividade para o acesso, facilidade de uso, segurança e a qualidade do serviço.
NP.11	Adequação dos assuntos relacionados à Tecnologia da Informação e Comunicação da UFPR à Lei Geral de Proteção de Dados Pessoais (LGPD).	Implementar as adequações de TIC, tais como aquelas relacionadas a sistemas de informação, bancos de dados, entre outros necessários ao atendimento dos requisitos impostos pela Lei nº 13.709, de 14 de agosto 2018.
NP.12	Prover soluções de cyber segurança para a UFPR.	Implementar soluções tecnológicas para proteger, monitorar e prevenir incidentes de segurança da informação, tais como ataques, invasões, acessos não autorizados, entre outros.

Fonte: PDTIC/UFPR 2022-2026, disponível em: <https://www.agtic.ufpr.br/portal/pdtic/>.

3.7. Parcelamento da Solução de TIC

3.7.1. A contratação prevê o agrupamento em função de aspectos técnicos da solução de TIC a ser contratada. O Lote 1 (lote único) é composto por equipamentos como firewall, access points, softwares, licenças, serviços, entre outros. Esse agrupamento é o mais adequado, caso contrário o parcelamento da solução, que teria como pressuposto a intenção de que vários fornecedores pudessem atender a UFPR, não se mostra gerencialmente e tecnicamente viável. Nessa abordagem, cada componente da solução, incluindo os serviços de garantia e suporte técnico, estaria sujeito à atuação conjunta de mais de um fornecedor, incluindo a oferta de equipamentos de diversas marcas e modelos, aumentando os riscos da contratação causados pela complexidade e problemas de compatibilidade dos equipamentos e softwares.

3.7.2. Dessa forma, os itens que integram o Lote 1 da presente contratação precisam ser totalmente compatíveis entre si, provendo a perfeita interoperabilidade da solução. O fornecimento de tais itens por diversos fabricantes acarretaria na impossibilidade de integração, de modo que os requisitos e necessidades não seriam atendidos, impedindo atingimento dos objetivos.

3.7.3. O parcelamento do Lote 1 em diversos itens pode acarretar prejuízos quanto à instalação, configuração e operacionalização de toda a solução, bem

como sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos e softwares a serem adquiridos. Além disso, a definição do agrupamento impacta na redução de custos operacionais, na capacidade técnica de manter a solução em operação, nos recursos humanos disponíveis para prestarem o devido apoio, curva de aprendizagem e no custo total de propriedade.

3.7.4. Após as análises realizadas, conclui-se que a adjudicação por lote único, além de respeitar as regulamentações e recomendações pertinentes, demonstrou ser a opção mais vantajosa para a Administração Pública. Ademais, existem vários fornecedores no mercado com plena capacidade de ofertar a solução almejada, proporcionando economicidade e atendendo aos princípios da competitividade e da isonomia.

3.8. Resultados e Benefícios a Serem Alcançados

3.8.1. Ao investir em uma solução de segurança da informação nativamente integrada e associada com a rede de dados sem fio da Universidade Federal do Paraná, com os componentes incluídos na presente contratação (firewall de nova geração para proteção de borda, pontos de acesso WLAN, controle de acesso seguro à rede, controle de acesso privilegiado, gerenciamento de identidade, proteção de e-mail, identificação e autenticação de acesso de visitantes e gestão centralizada de logs de auditoria), vários resultados positivos podem ser esperados. Abaixo a EPC lista os principais benefícios:

- Aumento da maturidade institucional em segurança da informação de acordo com as medições do PPSI ao investir em medidas consideradas prioritárias pelo referido Programa.
- Facilitação da gestão da segurança da informação e aumento da visibilidade das ameaças cibernéticas, incluindo condições de rastreamento dos pontos de vulnerabilidade.
- Proteção robusta e contínua com detecção e bloqueio contra ameaças avançadas providas da Internet via firewall de nova geração (NGFW), uma vez que oferecem defesa aprimorada contra malwares, ataques de negação de serviço (DDoS), explorações zero-day e outras ameaças cibernéticas sofisticadas.
- Controle granular de aplicações e de usuários via Firewall, no qual pode-se implementar políticas detalhadas de controle de acesso, permitindo ou bloqueando o uso de aplicações específicas com base em usuários, grupos ou dispositivos, melhorando a segurança e otimizando o uso dos recursos.
- Maior garantia de segurança para dispositivos móveis e remotos com os recursos de VPN e controles de acesso remoto incluídos no Firewall, possibilitando que a Universidade garanta que alunos, professores e demais colaboradores possam acessar a rede de forma segura, mesmo em ambientes externos, como em casa ou durante viagens.
- Segurança aprimorada no acesso à rede com NAT (Network Address Translation) e gerenciamento de identidade, com os quais a universidade poderá garantir que apenas dispositivos e usuários autorizados tenham acesso aos recursos, minimizando vulnerabilidades.
- Segmentação e isolamento de redes, uma vez que firewall + NAT permitirão segmentação eficiente das redes internas, isolando áreas críticas (como o datacenter, redes administrativas e laboratórios de pesquisa) de áreas comuns (como rede de visitantes e de acesso por alunos), reduzindo a superfície de ataque interno e invasão.
- Gerenciamento centralizado e simplificado com a integração dos diversos componentes em uma plataforma unificada, que permitirá um controle mais eficiente de todos os aspectos da segurança, com visibilidade consolidada e gestão de logs centralizada.
- Maior controle sobre acessos privilegiados, que proporcionará mais segurança na administração de usuários com permissões elevadas, reduzindo o risco de ataques internos.
- Proteção avançada de e-mails para filtragem de mensagens maliciosas, phishing e spams, fortalecendo a segurança das comunicações corporativas e reduzindo a níveis aceitáveis e gerenciáveis as contas comprometidas, protegendo os alunos, professores e demais colaboradores de golpes e de roubo de dados pessoais.
- Redução de riscos associados a visitantes com a solução de identificação e autenticação de visitantes, que garantirá que o acesso à rede por terceiros seja devidamente controlado e auditado, melhorando a segurança dos frequentes eventos e visitas promovidos na Universidade.
- Aumento da eficiência operacional com a integração nativa entre a rede sem fio (WLAN) e os outros componentes de segurança, com consequente simplificação da administração e do monitoramento, resultando em menos interrupções e uma infraestrutura mais estável e confiável.
- Respostas mais rápidas a incidentes com a gestão centralizada de logs de auditoria, que permitirá uma análise mais rápida e precisa de eventos de segurança, ajudando a identificar e mitigar incidentes com maior velocidade.
- Conformidade regulatória/legal facilitada, dado que a solução ajudará a Universidade a cumprir normas de segurança (incluindo a POSIC) e privacidade (como LGPD), oferecendo controle detalhado de acessos e atividades, além de relatórios de conformidade.
- Otimização de recursos de TI, pois a centralização da segurança em uma solução integrada reduz a complexidade operacional para a equipe de TI da Universidade, diminuindo o tempo gasto com múltiplas ferramentas e melhorando a capacidade de resposta a incidentes.
- Redução de custos a longo prazo, pois, embora o investimento inicial possa ser significativo, uma solução de segurança integrada pode reduzir os custos a longo prazo ao minimizar incidentes de segurança com ou sem vazamento de dados, evitar multas por não conformidade e diminuir a necessidade de correções emergenciais, além de reduzir a necessidade de várias soluções independentes.
- Melhor performance da rede sem fio integrada à infraestrutura de segurança, com otimização do desempenho da rede, proporcionando conectividade estável e segura para alunos, convidados e colaboradores.
- Prevenção de acessos não autorizados com o controle de identidade e autenticação robustos e confiáveis, garantindo que apenas usuários autenticados tenham acesso a serviços e sistemas, prevenindo acessos não autorizados.
- Melhoria na visibilidade e monitoramento de tráfego, dado que a integração de soluções de segurança proporcionará visibilidade abrangente sobre o tráfego da rede, permitindo detectar e reagir rapidamente a atividades suspeitas.

3.8.2. Esses benefícios fortalecerão a postura de segurança da Universidade Federal do Paraná, protegendo suas operações acadêmicas e administrativas.

4. REQUISITOS DA CONTRATAÇÃO

4.1. Requisitos de Negócio

4.1.1. As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (*Business Analysis Body of Knowledge* - Guia BABOK® v3), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição daquelas consideradas as mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

- Atender às demandas institucionais, em especial a segurança da informação e ampliação da capacidade de cobertura de rede sem fio da UFPR de maneira totalmente integrada e com gestão unificada;
- Padronizar as especificações e disposições contratuais;
- Permitir a agregação de um volume significativo de demanda e, com isso, obter potencialmente melhores ofertas tanto em termos financeiros quanto técnicos;
- Assegurar que os equipamentos possuam garantia e suporte ao longo de sua vida útil, de maneira a evitar ou reduzir ao máximo a indisponibilidade de equipamentos e serviços;
- Prover apoio tecnológico à continuidade dos serviços desenvolvidos em cada unidade da UFPR (princípio da Continuidade do Serviço Público).

4.2. Requisitos de Capacitação

4.2.1. Não faz parte do escopo da contratação a realização de capacitação técnica na utilização dos recursos relacionados ao objeto da presente contratação.

4.3. Requisitos Legais

4.3.1. O presente processo de contratação deve estar aderente à Constituição Federal e ao disposto nas legislações a seguir e outras aplicáveis:

- Lei nº 14.133, de 1º de abril de 2021, que estabelece normas gerais de licitação e contratação para as Administrações Públicas diretas, autárquicas e fundacionais da União, dos Estados, do Distrito Federal e dos Municípios;
- Decreto nº 7.174, de 12 de maio de 2010, que regulamenta a contratação de bens e serviços de informática e automação pela administração pública federal, direta ou indireta, pelas fundações instituídas ou mantidas pelo Poder Público e pelas demais organizações sob o controle direto ou indireto da União;
- Lei nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD);
- Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997;
- Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022, que dispõe sobre o processo de contratação de soluções de Tecnologia da Informação e Comunicação - TIC pelos órgãos e entidades integrantes do Sistema de Administração dos Recursos de Tecnologia da Informação - SISF do Poder Executivo Federal;
- Instrução Normativa SEGES/ME nº 65, de 7 de julho de 2021, que dispõe sobre o procedimento administrativo para a realização de pesquisa de preços para aquisição de bens e contratação de serviços em geral, no âmbito da administração pública federal direta, autárquica e fundacional.

4.4. Requisitos de Manutenção

4.4.1. A garantia deverá ser fornecida de acordo com os prazos definidos para cada um dos itens, contemplando reposição de equipamentos e peças danificadas, mão-de-obra de assistência técnica, e suporte, com atendimento remoto e *on-site* (no local de uso do equipamento quando, a critério da CONTRATANTE, for necessário) mediante abertura de chamado.

4.4.2. Os prazos de garantia serão contados a partir do recebimento definitivo dos equipamentos e softwares, conforme Tabela 3.

Tabela 3 – Prazos de Garantia

Descrição	Prazo de garantia	Tipo de garantia	Responsável
Equipamentos de firewall (itens 1, 3 e 5)	60 (sessenta) meses.	FortiCare PREMIUM	Fabricante
Equipamentos de pontos de acesso e injetor PoE (itens 7, 8, 9 e 10)	36 (trinta e seis) meses.	FortiCare PREMIUM	Fabricante
Soluções de softwares e licenças (itens 11, 12, 14, 15, 17, 19, 21, 23, 24, 26, 28)	36 (trinta e seis) meses.	FortiCare PREMIUM	Fabricante
Transceivers (itens 30, 31, 32 e 33)	60 (sessenta) meses.	FortiCare PREMIUM	Fabricante

4.4.3. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos e peças usadas, remanufaturadas, de demonstração ou acondicionadas em caixas violadas.

4.4.4. Os equipamentos deverão ser homologados e integrados em fábrica e ser entregues nas caixas lacradas pelo fabricante. Não serão aceitas adições ou subtrações de quaisquer componentes não originais de fábrica para adequação dos equipamentos.

4.4.5. A garantia dos bens e serviços que compõem a solução deverá ser prestada nos endereços indicados pela CONTRATANTE, distribuídos geograficamente no Estado do Paraná. A relação de locais, por município, que atualmente possuem unidades da UFPR a serem atendidas pela presente contratação, está disposta no ANEXO B - ENDEREÇOS DA UFPR NO PARANÁ do presente Termo de Referência.

4.4.6. O fabricante deve disponibilizar website ou software para consulta dos prazos de garantia dos bens e serviços. As informações de código do produto (*Serial Number*, *Service Tag*, entre outras denominações) devem ser facilmente localizadas e identificadas na parte externa do equipamento.

4.4.7. A CONTRATADA deverá substituir equipamentos, peças e componentes que apresentarem defeitos ou mau funcionamento em período de garantia por outros de especificação igual ou superior, novos, dentro dos prazos estipulados neste Termo de Referência.

4.4.8. Na ocorrência de defeitos, cada caso será tratado pontual e isoladamente. Quaisquer alegações por parte da CONTRATADA por ocasião do acionamento da garantia contra instalações (ambiente inadequado, rede elétrica, rede lógica, etc.) ou usuários (mau uso, etc.), devem ser comprovadas tecnicamente através de laudos detalhados e conclusivos, emitidos pelo fabricante do equipamento, sem ônus adicional à Contratante. Não serão admitidas omissões baseadas em suposições técnicas sem fundamentação ou baseadas na “experiência” dos técnicos envolvidos ou, ainda, alegações com base em exemplos de terceiros. Enquanto não for efetuado o laudo, e esse não demonstrar claramente os problemas alegados, a CONTRATADA deve prosseguir com o atendimento dos chamados, não cabendo direito de indenização ou compensação de qualquer espécie.

4.4.9. A substituição de componentes ou peças decorrentes da garantia será de responsabilidade única e exclusivamente do fabricante dos equipamentos, que ocorrerá durante o período de vigência da Garantia dos bens adquiridos, mesmo quando for necessário o transporte, por correio ou transportadora, de equipamentos e/ou peças ou ainda o traslado e a estada de técnicos pertencentes ao seu quadro de funcionários ou de sua rede de assistência técnica ou qualquer outro tipo de serviço necessário para o cumprimento da garantia. A substituição de componentes ou peças decorrentes da garantia não gera quaisquer ônus para a CONTRATANTE. Toda e qualquer peça ou componente consertado ou substituído, fica automaticamente garantido até o final do prazo de garantia do objeto.

4.4.10. Deverá ser garantido o acesso à *drivers*, manuais e *softwares* à CONTRATANTE, obrigatoriamente durante o período de garantia e até que o fabricante descontinue o suporte aos equipamentos.

4.4.11. O fabricante também deve disponibilizar atualização de novas versões de softwares, firmwares, sistemas operacionais e ferramentas de *troubleshooting*, decorrentes da evolução funcional ou correções do(s) anteriormente fornecido(s), durante o prazo da garantia dos equipamentos, sem quaisquer custos adicionais à CONTRATANTE.

4.4.12. A CONTRATANTE reserva-se o direito de aceitar ou não atualizações no *software* ou parte dele.

4.4.13. Especificamente para os itens de Serviço de configuração, o prazo de garantia é aquele estabelecido na Lei nº 8.078, de 11 de setembro de 1990 (Código de Defesa do Consumidor), conforme Tabela 4:

Tabela 4 – Prazos de Garantia fornecidos pela Contratada

Descrição	Prazo de garantia	Tipo de garantia	Responsável
Serviços de configuração (itens 2, 4, 6, 13, 16, 18, 20, 22, 25, 27, 29)	3 (três) meses.	Online/Remoto, Cobertura 8x5, NBD (Next Business Day)	Contratada

4.5. Requisitos Temporais

4.5.1. Os prazos e locais de entrega do objeto deverão ser efetivados, a contar do recebimento da Ordem de Fornecimento de Bens (OFB), emitida pela CONTRATANTE, conforme tabelas de prazos e locais de entrega descritos neste Termo de Referência.

4.6. Requisitos de Segurança e Privacidade

4.6.1. A CONTRATADA se obriga a tratar como informações sigilosas e privadas da UFPR quaisquer dados e informações relacionados à prestação dos serviços, utilizando-as apenas para as finalidades previstas no Contrato, não podendo revelá-las ou facilitar informações a terceiros;

4.6.2. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e seus meios de armazenamento, de que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais documentos;

4.6.3. Caso haja necessidade de substituição de dispositivos de armazenamento, a CONTRATADA se obriga a prover forma efetiva e segura de eliminação dos dados, de forma a manter o sigilo dos dados em alinhamento à Política de Segurança da Informação da UFPR e da Lei Geral de Proteção de Dados;

4.6.4. A fim de obter comprometimento formal da CONTRATADA sobre o sigilo dos dados e informações de uso da UFPR, bem como suas normas e políticas de segurança, a CONTRATADA deverá concordar e assinar, por meio de representante legal, Termo conforme padrão estabelecido pela UFPR no Anexo C – TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO;

4.6.5. A CONTRATADA se obriga a observar a Lei Geral de Proteção de Dados (LGPD);

4.6.6. A CONTRATADA se responsabilizará pelo ressarcimento por prejuízos causados pela inobservância dos itens acima ou outros de qualquer natureza, inclusive danos a terceiros;

4.6.7. Para demais situações de segurança não previstas neste Termo, a CONTRATADA se submeterá às políticas de segurança da informação e comunicação internas da CONTRATANTE;

4.6.8. A CONTRATANTE se compromete, em relação aos serviços sob contrato:

i. Comunicar imediatamente e oficialmente à CONTRATADA sobre incidentes e problemas de segurança ocorridos ou sobre possíveis riscos à segurança das informações e dados envolvendo os serviços contratados, assim como tomar providências, quando de sua competência, para a completa resolução dos incidentes e problemas ou mitigação dos riscos;

ii. Permitir e controlar o acesso de profissionais do fabricante e/ou da CONTRATADA às instalações da instituição, assim como em relação aos demais recursos envolvidos e sob responsabilidade da UFPR, mediante agendamento prévio com o solicitante responsável pelo chamado;

iii. Seguir as recomendações de uso do fabricante dos produtos envolvidos.

4.7. Requisitos Sociais, Ambientais e Culturais

4.7.1. Quanto aos profissionais da CONTRATADA caberá:

a) Agir de maneira ética e profissional;

b) Manter conduta compatível com a moralidade administrativa;

c) Ser cortês, ter urbanidade, disponibilidade e atenção, respeitando a capacidade e as limitações individuais de todos os usuários do serviço público, sem qualquer espécie de preconceito ou distinção de raça, sexo, nacionalidade, cor, idade, religião, cunho político e posição social;

d) Tratar cuidadosamente os usuários dos serviços, aperfeiçoando o processo de comunicação e contato com o público;

e) Contribuir para a conservação da harmonia e organização do ambiente de trabalho, mantendo-o limpo e em perfeita ordem, seguindo os métodos mais adequados à sua organização e distribuição;

f) Manter-se atualizado com as instruções, as normas de serviço e a legislação pertinentes à UFPR;

g) Exercer suas atribuições com rapidez, perfeição e rendimento;

h) Facilitar a fiscalização de todos seus atos ou serviços por quem de direito;

i) Repassar ao fiscal técnico ou ao demandante o registro das ações executadas, mantendo a documentação organizada e em local acessível pelos mesmos, não sendo necessário o pedido para tal.

4.7.2. O trânsito de veículos da CONTRATADA estará sujeito às normas e procedimentos internos da UFPR;

4.7.3. Os profissionais da CONTRATADA, quando nas dependências da UFPR, deverão apresentar uniforme e possuir identificação funcional individualizada através de crachás, a encargo da CONTRATADA, sem custos adicionais para a CONTRATANTE;

4.7.4. A CONTRATADA, se cabível, deverá fornecer a seus funcionários EPI (Equipamento de Proteção Individual) e EPC (Equipamento de Proteção Coletivo), bem como todas as ferramentas e instrumentos necessários à execução dos serviços contratados, sem custos adicionais à CONTRATANTE.

4.7.5. Quanto aos produtos:

i. Devem ser acondicionados em embalagem individual adequada, com o menor volume possível, que utilize materiais recicláveis, de forma a garantir a máxima proteção durante o transporte e o armazenamento e permita o descarte sustentável;

ii. Cabe exclusivamente à CONTRATADA remover, às suas expensas, todo o material que estiver em desacordo com as especificações básicas e/ou aquele

em que for constatado dano em decorrência de transporte ou acondicionamento, providenciando a substituição do mesmo por material adequado às especificações.

4.7.6. Em relação à questão ambiental e política de descarte de resíduos:

i. 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 especial a responsabilidade compartilhada pelo ciclo de vida do produto.

4.8. Requisitos da Arquitetura Tecnológica

4.8.1. Os equipamentos e softwares deverão observar integralmente os requisitos de arquitetura tecnológica descritos no Anexo A - ESPECIFICAÇÕES TÉCNICAS DOS ITENS.

4.9. Requisitos de Projeto e de Implementação

4.9.1. Os equipamentos e softwares deverão observar integralmente os requisitos de projeto e de implementação definidos pelo fabricante.

4.10. Requisitos de Implantação

4.10.1. Os equipamentos e softwares deverão observar integralmente os requisitos de implantação, instalação e fornecimento definidos pelo fabricante.

4.11. Requisitos de Garantia, Manutenção e Assistência Técnica

4.11.1. Os serviços estão sujeitos a serem refeitos caso não atendam a necessidade e requisitos descritos neste Termo de Referência, sem ônus adicional para a CONTRATANTE.

4.11.2. Os meios de acionamento para atendimento aos requisitos de garantia são os mesmos para acionamento dos demais serviços previstos.

4.12. Requisitos de Experiência Profissional e Formação da Equipe

4.12.1. 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.

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

4.13. Requisitos de Metodologia de Trabalho

4.13.1. Os requisitos de metodologia de trabalho estão descritos no "Modelo de Execução do Contrato".

4.14. Requisitos de Segurança da Informação e Privacidade

4.14.1. A CONTRATADA deverá observar integralmente os requisitos de Segurança da Informação e Privacidade, com a finalidade de garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações e a privacidade dos dados, quando aplicáveis.

a) A CONTRATADA se obriga a tratar como informações sigilosas e privadas da UFPR quaisquer dados e informações relacionados à prestação dos serviços, utilizando-as apenas para as finalidades previstas no Contrato, não podendo revelá-las ou facilitar informações a terceiros.

b) A CONTRATADA deve manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias que venha a ter conhecimento durante a execução dos serviços, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela CONTRATANTE a tais dados e documentos.

c) A CONTRATADA se obriga a obedecer a Lei Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD), e manter atualizadas as informações sobre o Encarregado pelo Tratamento de Dados Pessoais e canais de contato.

d) A fim de obter comprometimento formal da CONTRATADA sobre o sigilo dos dados e informações de uso da UFPR, bem como suas normas e políticas de segurança, a CONTRATADA deverá concordar e assinar, por meio de representante legal, o Termo de Compromisso e Manutenção de Sigilo constante do Anexo C deste Termo de Referência.

e) A fim de identificar os funcionários prestadores de serviço na UFPR, a CONTRATADA se obriga a coletar a assinatura de seus profissionais no Termo de Compromisso e Manutenção de Sigilo, conforme Termo de Ciência disposto no Anexo D. O referido documento deverá ser apresentado sempre que houver a inclusão de novos funcionários/empregados atuantes na execução dos serviços. De qualquer forma, a CONTRATADA não pode se escusar de atos contrários ao estabelecido no Termo de Compromisso e Manutenção de Sigilo cometidos por seus funcionários.

f) A CONTRATADA se obriga a disponibilizar sua política de segurança da informação conforme especificações neste Termo de Referência, devendo comunicar a CONTRATANTE sempre que houver alterações na mesma.

g) A CONTRATADA se responsabilizará pelo ressarcimento por prejuízos causados pela inobservância dos itens acima ou outros de qualquer natureza, inclusive danos a terceiros.

h) A CONTRATADA estará sujeita a sanções administrativas pelo descumprimento de cada um dos requisitos de segurança da informação e de privacidade especificados neste Termo de Referência.

i) A CONTRATANTE se compromete em relação aos serviços sob contrato:

i. Comunicar imediatamente e oficialmente à CONTRATADA sobre incidentes e problemas de segurança ocorridos ou sobre possíveis riscos à segurança das informações e dados envolvendo os serviços contratados, assim como tomar providências, quando de sua competência, para a completa solução dos incidentes e problemas ou mitigação dos riscos;

ii. Permitir e controlar o acesso de profissionais da CONTRATADA às instalações da instituição, assim como em relação aos demais recursos envolvidos e sob responsabilidade da UFPR;

iii. Seguir as recomendações de uso do fabricante dos produtos envolvidos.

4.14.2. As contratações de soluções de TIC devem atender às normas específicas dispostas no Guia de Requisitos e de Obrigações quanto à Segurança da Informação e Privacidade, publicado pelo Órgão Central do SISP, em alinhamento ao art. 8º, § 2º da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

4.14.3. Demais questões relativas à Segurança da Informação não previstas neste Termo de Referência e seus anexos obedecerão à Política de Segurança da Informação e Comunicação da UFPR e outras normas internas relacionadas à TI ou ainda, caso não previstas nestas, serão negociados entre as partes,

sempre primando pelas melhores práticas de segurança.

4.15. Sustentabilidade

4.15.1. Foram consultados o Guia Nacional de Contratações Sustentáveis da AGU (7ª edição), os critérios de sustentabilidade ambiental contidos no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República. No entanto não foram identificados outros critérios de sustentabilidade além daqueles eventualmente inseridos na descrição do objeto.

4.15.2. Além disso, devem ser atendidos os requisitos previstos na Lei nº 12.305, de 2 de agosto de 2010, que institui a Política Nacional de Resíduos Sólidos e Decreto nº 10.936, de 12 de janeiro de 2022, que regulamenta a Lei nº 12.305.

4.16. Indicação de marcas ou modelos (Art. 41, inciso I, da Lei nº 14.133, de 2021)

4.16.1. Na presente contratação será admitida a indicação da seguinte marca, características ou modelos, de acordo com as justificativas contidas nos Estudos Técnicos Preliminares: Fortinet.

4.16.2. A indicação da marca Fortinet observa o princípio da padronização, considerada a compatibilidade de especificações estéticas, técnicas ou de desempenho, nos termos do art. 43 da Lei nº 14.133, de 2021, e do art. 9º, inciso I, alínea b, da IN Seges/ME nº 81, de 2022.

4.17. Diligências e provas de conceito

4.17.1. Poderão ser realizadas, sempre que necessárias, diligências, para fins de comprovação de atendimento das especificações técnicas ou para dirimir quaisquer outras dúvidas, quando aplicável;

4.17.2. Não será realizada, neste certame, Prova de Conceito com as licitantes.

4.18. Da exigência de carta de solidariedade

4.18.1. Não será exigida carta de solidariedade emitida pelo fabricante na presente contratação. No entanto, será solicitada a comprovação de que a empresa está relacionada como *partner*, caso não seja ela própria o fabricante, atestando que a CONTRATADA é representante autorizada e está habilitada a comercializar, prestar serviços de instalação, configuração e suporte técnico aos equipamentos e softwares do fabricante, sem prejuízo da garantia.

4.19. Subcontratação

4.19.1. Não é admitida a subcontratação do objeto contratual.

4.20. Alteração Subjetiva

4.20.1. É admissível a fusão, cisão ou incorporação da CONTRATADA com/em outra pessoa jurídica, desde que sejam observados pela nova pessoa jurídica todos os requisitos de habilitação exigidos na licitação original; sejam mantidas as demais cláusulas e condições do contrato; não haja prejuízo à execução do objeto pactuado e haja a anuência expressa da Administração à continuidade do contrato.

4.21. Garantia da Contratação

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

4.22. Informações Relevantes para o dimensionamento e Apresentação da Proposta

4.22.1. A justificativa fundamentando a definição e quantidade dos itens encontra-se no Estudo Técnico Preliminar, apêndice deste Termo de Referência.

5. PAPÉIS E RESPONSABILIDADES

5.1. Obrigações da CONTRATANTE

5.1.1. Nomear Gestor e Fiscais Técnico, Administrativo e Requisitante do contrato para acompanhar e fiscalizar a execução do contrato;

5.1.2. Encaminhar formalmente a demanda por meio de Ordem de Serviço ou de Fornecimento de Bens, de acordo com os critérios estabelecidos no Termo de Referência;

5.1.3. Receber o objeto fornecido pela CONTRATADA que esteja em conformidade com a proposta aceita, conforme inspeções realizadas;

5.1.4. Aplicar à CONTRATADA as sanções administrativas regulamentares e contratuais cabíveis, comunicando ao órgão gerenciador da Ata de Registro de Preços, quando aplicável;

5.1.5. Liquidar o empenho e efetuar o pagamento à CONTRATADA, dentro dos prazos preestabelecidos em contrato;

5.1.6. Comunicar à CONTRATADA todas e quaisquer ocorrências relacionadas com o fornecimento da solução de TIC;

5.1.7. Realizar, no momento da licitação e sempre que possível e aplicável, diligências, para fins de comprovação de atendimento das especificações técnicas ou para dirimir quaisquer outras dúvidas;

5.1.8. Repassar à CONTRATADA as informações sobre o ambiente de trabalho da CONTRATANTE que possam ser relevantes para a prestação dos serviços;

5.1.9. Gerenciar os licenciamentos adquiridos via plataforma/sistema disponibilizado pelo Fabricante.

5.2. Obrigações da CONTRATADA

5.2.1. Indicar formalmente preposto apto a representá-la junto à CONTRATANTE, que deverá responder pela fiel execução do contrato;

5.2.2. Atender prontamente quaisquer orientações e exigências da Equipe de Fiscalização do Contrato, inerentes à execução do objeto contratual;

5.2.3. Reparar quaisquer danos diretamente causados à CONTRATANTE ou a terceiros por culpa ou dolo de seus representantes legais, prepostos ou empregados, em decorrência da relação contratual, não excluindo ou reduzindo a responsabilidade da fiscalização ou o acompanhamento da execução dos

serviços pela Contratante;

5.2.4. Propiciar todos os meios necessários à fiscalização do contrato pela CONTRATANTE, cujo representante terá poderes para sustar o fornecimento, total ou parcial, em qualquer tempo, desde que motivadas as causas e justificativas desta decisão;

5.2.5. Manter, durante toda a execução do contrato, as mesmas condições da habilitação;

5.2.6. Quando especificada, manter, durante a execução do contrato, equipe técnica composta por profissionais devidamente habilitados, treinados e qualificados para fornecimento da solução de TIC;

5.2.7. Executar o objeto do certame em estreita observância dos ditames estabelecidos pela Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais – LGPD);

5.2.8. Não veicular publicidade ou qualquer outra informação acerca da prestação dos serviços do contrato, sem prévia autorização da Contratante;

5.2.9. Não fazer uso das informações prestadas pela Contratante para fins diversos do estrito e absoluto cumprimento do contrato em questão;

5.2.10. Aceitar e assinar o Termo de Compromisso e Manutenção de Sigilo (Anexo C), comprometendo-se a dar ciência do mesmo aos seus empregados, sobretudo àqueles com envolvimento direto na prestação dos serviços com a Contratante.

5.3. 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:

- As formas de comunicação entre os envolvidos, a exemplo de ofício, telefone, e-mail, ou sistema informatizado, quando disponível; e
- Definição dos eventos a serem reportados ao órgão gerenciador, com a indicação de prazo e responsável.

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

- 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 pela CONTRATADA; e
- As regras para a substituição da solução registrada na Ata de Registro de Preços, em função de fatores supervenientes que tornem necessária e imperativa a substituição da solução tecnológica.

6. MODELO DE EXECUÇÃO DO CONTRATO

6.1. O fornecimento dos itens será parcelado, em quantidades variáveis, conforme a necessidade e disponibilidade orçamentária da UFPR, durante o período de 12 (doze) meses, contados da assinatura da UFPR na ata de registro de preços.

6.2. Rotinas de Execução

6.2.1. Do Encaminhamento Formal de Demandas

6.2.1.1. Documentos Necessários: para fins de acompanhamento do contrato, valem as seguintes definições e documentos:

- Ordem de Fornecimento de Bens/Serviços: o documento utilizado para solicitar à CONTRATADA o fornecimento de bens relativos ao objeto desta contratação será a Nota de Empenho;
- Declaração de Garantia: documento a ser preenchido pela CONTRATADA e entregue na ocasião da assinatura da Ata de Registro de Preços, conforme Anexo F – DECLARAÇÃO DE GARANTIA;
- Nota(s) Fiscal(is): notas fiscais emitidas pela CONTRATADA e aprovadas pela CONTRATANTE.

6.2.1.2. Regras Gerais:

- A CONTRATADA cumprirá as instruções complementares da UFPR quanto à execução e horário de realização do serviço, permanência e circulação de seu(s) técnico(s) nas dependências da UFPR;
- A ação ou omissão total ou parcial da fiscalização da UFPR não eximirá a CONTRATADA da total responsabilidade pela execução do objeto do Contrato.

6.2.1.3. Relatórios:

6.2.1.3.1. A CONTRATADA se obriga a prestar relatórios eventuais com informações pertinentes às aquisições, sempre que solicitado pelos Fiscais ou Gestores da Ata, nos prazos e formas previamente negociados entre UFPR e CONTRATADA, desde que tenham relação com o fornecimento dos bens e prestação dos serviços da garantia.

6.3. Forma de execução e acompanhamento do contrato

6.3.1. Aceite dos Produtos

6.3.1.1. Os equipamentos descritos no Anexo A - ESPECIFICAÇÕES TÉCNICAS DOS ITENS deste Termo de Referência, deverão ser entregues nos prazos e locais estipulados.

6.3.1.2. O recebimento de equipamentos em entrega ou em substituição compreenderá 2 (dois) momentos:

- O recebimento provisório, onde será realizada a conferência quantitativa (porém, não limitada a esse requisito) dos produtos no momento da chegada do equipamento na Universidade;
- O recebimento definitivo, que poderá ser realizado em data posterior à do recebimento provisório, após conferência técnica do produto com base nas exigências especificadas a seguir:

Tabela 5 – Aceite dos Produtos

Aceite	Prazo	Observações
--------	-------	-------------

Recebimento definitivo	Até 30 (trinta) dias corridos a partir do recebimento provisório.	Caso não haja emissão de documento comprobatório até o limite aqui estipulado, considerar-se-á automaticamente aceito pela CONTRATANTE.
------------------------	---	---

6.3.1.3. Os itens adquiridos serão, inicialmente, recebidos pela unidade requisitante de forma provisória, mediante assinatura de documento comprobatório por parte da CONTRATANTE. A partir da data de recebimento provisório, passa-se a contar o prazo para o recebimento definitivo.

6.3.1.4. Quando constatada alguma inconformidade com os quantitativos ou com os produtos no recebimento provisório ou durante o período compreendido entre o recebimento provisório e o recebimento definitivo, a UFPR notificará a CONTRATADA, que deverá corrigir quantitativos ou substituir aqueles com defeito de fabricação ou com inconformidade por outro de especificação igual ou superior, novo, nos prazos estipulados no Edital, contados da notificação, sem ônus para a UFPR.

6.3.1.5. Verificada a compatibilidade entre o objeto contratado e o executado, bem como a qualidade e a integridade dos materiais e dos serviços prestados, incluindo os ajustes e correções necessárias, o Fiscal Requisitante ou Fiscal Técnico assinará o recebimento definitivo, por meio do ateste (assinatura) da nota fiscal dos produtos. Sendo desatendida qualquer determinação da especificação contida neste Termo de Referência, o Requisitante solicitará que o produto seja substituído, sem quaisquer ônus para a UFPR, notificando o fato à CONTRATADA por e-mail ou através de sistema eletrônico de tratamento de chamados, observando os prazos estipulados no presente Termo.

6.3.1.6. Especificamente para os itens de softwares e licenças, a partir do recebimento da Nota de Empenho enviada pela unidade solicitante (Agência de Tecnologia da Informação e Comunicação - AGTIC), a CONTRATADA deverá agendar a entrega com a equipe da Coordenadoria de Serviços e Infraestrutura de TIC (AGTIC/CSI), através do e-mail csi@ufpr.br, com cópia para agtic@ufpr.br. Opcionalmente, pelo telefone (41) 3361-3321. No caso de a entrega das licenças ocorrer por meios digitais, estas devem ser creditadas para o e-mail csi@ufpr.br.

6.3.2. Locais de Entrega

6.3.2.1. Os bens e serviços que compõem a solução deverão ser entregues/prestados em diversos Campi da UFPR, indicados pela CONTRATANTE na Nota de Empenho, distribuídos geograficamente no Estado do Paraná.

6.3.2.2. A relação de locais, por município, que atualmente possuem unidades da UFPR a serem atendidas pela presente contratação, está disposta no ANEXO B - ENDEREÇOS DA UFPR NO PARANÁ do presente Termo de Referência.

6.3.2.3. As aquisições dos equipamentos, em sua maioria, deverão ocorrer para Curitiba, podendo ser adquiridas para unidades descentralizadas em menor quantidade. A AGTIC fará o controle dessas solicitações a fim de orientar a unidade adquirente quanto à informação do local de entrega na Nota de Empenho.

6.3.2.4. Para efeitos de entregas à Agência de Tecnologia da Informação e Comunicação, a AGTIC está localizada no Centro Politécnico, à Rua Coronel Francisco Heráclito dos Santos, nº 100, Jardim das Américas – Curitiba/PR, CEP 81531-980, no 4º andar do Prédio de Administração.

6.3.2.5. A Nota de Empenho indicará a quantidade, itens da Ata, endereço de entrega, nome do responsável pelo recebimento, acompanhado do e-mail e/ou telefone para contato.

6.3.2.6. A CONTRATADA deve prever todos os custos necessários para a entrega dos bens e serviços, não sendo possível em nenhuma hipótese o pagamento de valor adicional ao empenhado.

6.3.2.7. Para fins de melhoria no processo logístico de entrega dos equipamentos, em diferentes localidades, é exigido que a CONTRATADA inclua etiqueta na embalagem (caixa) com informações relevantes incluindo, no mínimo, número de empenho, unidade adquirente e contato do responsável.

6.3.3. Prazos de Entrega

6.3.3.1. Para fins de entrega dos bens e prestação dos serviços relacionados à garantia, ficam estipuladas as regiões e endereços constantes do Anexo B - ENDEREÇOS DA UFPR NO PARANÁ deste Termo de Referência.

6.3.3.2. Ficam estipulados e caracterizados os seguintes prazos a serem cumpridos pela CONTRATADA para entrega dos itens em aquisição:

Tabela 6 – Prazos de Entrega

Itens	Prazo de entrega padrão	Extensões de prazo de entrega	Prazo de substituição padrão	Extensões de prazo de substituição
Equipamentos de firewall (itens 1, 3 e 5)	90 (noventa) dias corridos a partir da ordem de serviço (empenhamento).	30 (trinta) dias corridos mediante aprovação expressa da CONTRATANTE.	30 (trinta) dias corridos a partir da comunicação.	10 (dez) dias corridos mediante aprovação expressa da CONTRATANTE.
Equipamentos de pontos de acesso e injetor PoE (itens 7, 8, 9 e 10)	90 (noventa) dias corridos a partir da ordem de serviço (empenhamento).	30 (trinta) dias corridos mediante aprovação expressa da CONTRATANTE.	30 (trinta) dias corridos a partir da comunicação.	10 (dez) dias corridos mediante aprovação expressa da CONTRATANTE.
Soluções de softwares e licenças (itens 11, 12, 14, 15, 17, 19, 21, 23, 24, 26, 28)	10 (dez) dias corridos a partir da ordem de serviço (empenhamento).	5 (cinco) dias corridos mediante aprovação expressa da CONTRATANTE.	5 (cinco) dias corridos a partir da comunicação, caso se aplique.	5 (cinco) dias corridos mediante aprovação expressa da CONTRATANTE.

Serviços de configuração (itens 2, 4, 6, 13, 16, 18, 20, 22, 25, 27, 29)	10 (dez) dias corridos a partir da ordem de serviço (empenhamento).	5 (cinco) dias corridos mediante aprovação expressa da CONTRATANTE.	5 (cinco) dias corridos a partir da comunicação, caso se aplique.	5 (cinco) dias corridos mediante aprovação expressa da CONTRATANTE.
Transceivers (itens 30, 31, 32 e 33)	30 (trinta) dias corridos a partir da ordem de serviço (empenhamento).	10 (dez) dias corridos mediante aprovação expressa da CONTRATANTE.	15 (quinze) dias corridos a partir da comunicação.	5 (cinco) dias corridos mediante aprovação expressa da CONTRATANTE.

6.3.3.3. Caso o prazo de entrega padrão não seja suficiente, a CONTRATADA poderá requerer formalmente a extensão de prazo, devendo a CONTRATANTE avaliar as justificativas apresentadas e, dentro do aceitável e do bom senso, conceder ou negar as extensões de prazo solicitadas.

6.3.3.4. A CONTRATADA deverá informar à CONTRATANTE, quando da entrega dos equipamentos, com no mínimo 2 (dois) dias úteis de antecedência, ficando a CONTRATADA responsável pelo transporte e entrega dos equipamentos.

6.3.3.5. Não serão aceitas entregas parciais de um mesmo empenho, ou seja, todo o produto/serviço deverá ser prestado dentro dos prazos definidos neste Termo de Referência.

6.3.3.6. A CONTRATADA não será penalizada por atrasos nos prazos quando por culpa da CONTRATANTE ou por atrasos em decorrência de qualquer eventualidade que ocorra por motivo de força maior, imprevisível ou de difícil previsão, alheia à vontade de ambas as partes. De qualquer forma, a CONTRATADA se obriga a notificar a CONTRATANTE, requerendo as extensões de prazo e justificando claramente os motivos, que serão alvo de avaliação pela UFPR antes de recusa ou aceitação.

6.4. Formas de transferência de conhecimento

6.4.1. Não será necessária transferência de conhecimento além daquelas já previstas na descrição dos itens de serviços de configuração, conforme Anexo A – ESPECIFICAÇÕES TÉCNICAS DOS ITENS.

6.5. Procedimentos de transição e finalização do contrato

6.5.1. Não serão necessários procedimentos de transição e finalização do contrato devido às características do objeto.

6.6. Quantidade mínima de bens ou serviços para comparação e controle

6.6.1. Cada OFB conterá a quantidade a ser fornecida, incluindo a sua localização e o prazo, conforme definições deste Termo de Referência.

6.6.2. O fornecimento dos itens será parcelado, em quantidades variáveis, conforme a necessidade e disponibilidade orçamentária da UFPR, durante o período de vigência da Ata de Registro de Preços.

6.7. Mecanismos formais de comunicação

6.7.1. São definidos como mecanismos formais de comunicação, entre a CONTRATANTE e a CONTRATADA, os seguintes:

Tabela 7 – Formas de Comunicação e Documentos

Forma de Comunicação ou Documento	Descrição e aplicação
Telefone	Pode ser utilizado para alinhamentos, esclarecimento de dúvidas e outras demandas que possam ser tratadas informalmente e com propósito de dar agilidade às tratativas. A CONTRATADA deverá informar os seus números de contato, assim como seus demais canais de comunicação e mantê-los sempre atualizados durante a vigência contratual.
E-mail	Deve ser utilizado para comunicações relativas a convites/convocações para reuniões, atualização de informações relevantes ao Contrato e assuntos diversos que mereçam ser documentados, para fins de auditoria, e que não estejam previstos nas demais formas elencadas. Devem ser utilizados única e exclusivamente endereços de e-mail institucionais, de ambas as partes.

Atendimento (chamado técnico)	Registro de solicitações e atendimentos da UFPR para suporte e providências quanto a incidentes, eventos, problemas, ocorrências relativas ao objeto do Contrato via sistema eletrônico de tratamento de chamados da CONTRATADA, devendo constar do registro das solicitações as seguintes informações mínimas: - Identificação do solicitante da UFPR; - Identificação do(s) técnico(s) envolvidos no atendimento; - Número da solicitação; - Assunto da solicitação; - Descrição da solicitação; - Datas de abertura, acompanhamentos e encerramento da solicitação; - Relato dos acompanhamentos (tratativas) dadas ao atendimento; - Anexos envolvidos nas tratativas do chamado. Toda comunicação entre solicitante e técnicos, independentemente do meio utilizado, envolvendo a resolução de problemas relativos a garantia, deverá ter seu conteúdo registrado pela CONTRATADA em chamado técnico. O protocolo de atendimento deverá ser informado ao solicitante no momento da abertura do chamado.
Ata de Reunião	Documento de registro formal dos assuntos tratados em reuniões (informações, negociações, explanações, acordos, tratados, pendências, responsabilidades, entre outras) entre UFPR e CONTRATADA, relativamente ao Contrato, a ser criado sempre por servidor da UFPR. A ata de reunião deverá conter, no mínimo, as seguintes informações: - Identificação do contrato à qual se refere a reunião; - Data e local da reunião; - Agenda da reunião (pauta); - Enumeração dos assuntos tratados; - Descrição dos assuntos tratados; - Resumo das pendências e responsabilidades assumidas pelas partes; - Identificação dos participantes (nome, órgão/empresa, assinatura).
Ofício	Documento para formalização e evidência de demandas que ensejem acordos, tratados, avisos, comunicados, dentre outras, a ser utilizado por ambas as partes, sempre que houver o entendimento ou a necessidade de evidenciar tais fatos e que necessitem de tramitação para ciência e aprovação nas partes.
Reunião Virtual ou Presencial	Reuniões realizadas presencialmente ou por meio da Internet, com recursos de comunicação, para tratamento de assuntos diversos e relevantes para tomada de decisões relativas ao contrato. Independentemente de ser presencial ou virtual, demanda a elaboração de ata de reunião.
Relatórios	Relatórios eventuais com informações pertinentes às aquisições, sempre que solicitados pelos Fiscais ou Gestores da Ata, nos prazos e formas previamente negociados entre UFPR e CONTRATADA.

6.8. Manutenção de Sigilo e Normas de Segurança

6.8.1. A CONTRATADA deverá manter sigilo absoluto sobre quaisquer dados e informações contidos em quaisquer documentos e mídias, incluindo os equipamentos e softwares, de que venha a ter conhecimento durante a execução do contrato, não podendo, sob qualquer pretexto, divulgar, reproduzir ou utilizar, sob pena de lei, independentemente da classificação de sigilo conferida pela Contratante a tais documentos.

6.8.2. O Termo de Compromisso e Manutenção de Sigilo, contendo declaração de manutenção de sigilo e respeito às normas de segurança vigentes na entidade, a ser assinado pelo representante legal do Contratado, encontra-se no ANEXO C – TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO.

6.9. Papéis e Responsabilidades

6.9.1. Para a execução do objeto da presente contratação deverão ser designados os seguintes papéis e respectivas responsabilidades:

Tabela 8 – Papéis e Responsabilidades

Papel	Responsabilidades
Preposto	Representante da CONTRATADA, por esta indicado e formalmente nomeado, responsável por acompanhar a execução do objeto e atuar como interlocutor principal junto à UFPR, incumbido de receber, diligenciar, encaminhar e responder as principais questões técnicas, legais e administrativas referentes ao andamento contratual.
Gestor Administrativo da Ata	Servidor com atribuições gerenciais, técnicas e operacionais relacionadas ao processo de gestão do contrato, indicado por autoridade competente da UFPR para gerir administrativamente o contrato, divulgar informações quanto aos procedimentos para compra, autorizar as solicitações de compras, orientar quanto à fiscalização dos bens/serviços contratados, controlar os quantitativos registrados, solicitar apoio e parecer do Gestor Técnico ou dos fiscais quando necessário, dentre outras atribuições legais e normatizadas pela UFPR.
Gestor Técnico da Ata	Servidor representante da Área de Tecnologia da Informação, indicado pela autoridade competente dessa área, na UFPR, para acompanhar e analisar tecnicamente a gestão do contrato.

Fiscal Técnico da Área de TIC	Servidor de Tecnologia da Informação, com competência para fiscalizar tecnicamente a execução do objeto, lotado na unidade que solicitou a compra. Deve auxiliar os Requisitantes quanto às dúvidas técnicas e interlocuções junto à CONTRATADA; demandar serviços técnicos à CONTRATADA e à AGTIC; prestar acompanhamento e aprovação da execução dos serviços; acompanhar e analisar os relatórios de atendimentos de garantia; acompanhar e fiscalizar a execução dos serviços; interceder junto ao preposto da CONTRATADA; avaliar e aceitar produtos e serviços concernentes à solução de TIC; demandar laudos técnicos; notificar o Gestor da Ata sobre o descumprimento de cláusulas contratuais, dentre outras atribuições legais e normatizadas pela UFRP. No caso de não haver profissional de TIC no Setor, Pró-Reitoria, Superintendência ou Campus, responderá pelo papel, o servidor que for indicado pela AGTIC para a função de Fiscal Técnico da Área de TIC.
Fiscal Administrativo da Ata	Verificar as certidões de regularidade da CONTRATADA; solicitar o fornecimento de bens à CONTRATADA; verificar prazos de entrega; conferir nota fiscal e outros documentos entregues pela CONTRATADA; instruir processo de sanção administrativa com auxílio dos fiscais requisitantes e técnicos quando necessário; encaminhar a liberação de pagamento à CONTRATADA após recebimento definitivo, dentre outras atribuições legais e normatizadas pela UFRP.
Fiscal Requisitante da Ata	Caberá a qualquer servidor que solicitar a compra de equipamentos fiscalizar os bens e serviços contratados, observando os prazos e as obrigações dispostas no Termo de Referência, na Declaração de Garantia e na ARP, incluindo atestar o recebimento definitivo (com o auxílio do fiscal técnico, quando necessário) dos bens adquiridos que estiverem em conformidade com o objeto contratado, sua marca, modelo e especificações, solicitar serviços de garantia, encaminhar demandas de serviços aos fiscais técnicos ou à AGTIC, dentre outras atribuições afins.
Equipe técnica da AGTIC/CSI	Técnicos e Analistas de Tecnologia da Informação da Coordenadoria de Serviços e Infraestrutura de TIC (CSI), responsáveis por auxiliar o Fiscal Técnico em suas atribuições, auxiliar na identificação de falhas nos equipamentos e softwares, e proceder os ajustes, correções ou substituições necessárias por parte da CONTRATANTE para a correta operação da solução.

6.9.2. Opcionalmente, poderão ser indicados pela autoridade competente Suplentes para os Gestores e Fiscais do contrato com a missão de assumir suas funções e responsabilidades em casos de ausências ou faltas. Em caso de destituição do titular, os suplentes assumirão suas atribuições.

6.9.3. As indicações de Gestor Administrativo da Ata e de Gestor Técnico da Ata serão de responsabilidade da Coordenadoria de Licitações e Contratações (CLIC) e da Agência de Tecnologia da Informação e Comunicação (AGTIC), respectivamente. Já as indicações dos Fiscais Requisitante, Técnico (quando houver profissional de TIC disponível na unidade solicitante) e Administrativo serão de responsabilidade dos Setores, Pró-Reitorias, Superintendências ou Unidades que requisitarem a compra de equipamentos. Os Gestores e Fiscais da AGTIC para a Ata serão nomeados por meio de ato do Pró-Reitor de Administração ou pessoa delegada.

6.9.4. As responsabilidades aqui especificadas não excluem aquelas estabelecidas na Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

7. MODELO DE GESTÃO DO CONTRATO

7.1. O gerenciamento da ata de registro de preços será responsabilidade da **Agência de Tecnologia de Informação e Comunicação**.

7.2. A ata de registro de preços deverá ser executada 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.

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 a CONTRATADA 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.

Fiscalização

7.6. A execução do contrato deverá ser acompanhada e fiscalizada pelo(s) fiscal(is) do contrato, ou pelos respectivos substitutos (Lei nº 14.133, de 2021, art. 117, caput), nos termos do art. 33 da IN SGD nº 94, de 2022, observando-se, em especial, as rotinas a seguir.

Fiscalização Técnica

7.7. O fiscal técnico do contrato, além de exercer as atribuições previstas no art. 33, II, da IN SGD nº 94, de 2022, acompanhará a execução do contrato, para que sejam cumpridas todas as condições estabelecidas no contrato, de modo a assegurar os melhores resultados para a Administração. (Decreto nº 11.246, de 2022, art. 22, VI);

7.8. O fiscal técnico do contrato anotará no histórico de gerenciamento do contrato todas as ocorrências relacionadas à execução do contrato, com a descrição do que for necessário para a regularização das faltas ou dos defeitos observados. (Lei nº 14.133, de 2021, art. 117, §1º, e Decreto nº 11.246, de 2022, art. 22, II);

7.9. Identificada qualquer inexistência 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. 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);

7.11. 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);

7.12. 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

7.13. 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 da CONTRATADA, 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);

7.14. 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

7.15. 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);

7.16. O gestor do contrato acompanhará a manutenção das condições de habilitação do contratado, para fins de empenho de despesa e pagamento, e anotará os problemas que obstem o fluxo normal da liquidação e do pagamento da despesa no relatório de riscos eventuais. (Decreto nº 11.246, de 2022, art. 21, III);

7.17. 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);

7.18. 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);

7.19. 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);

7.20. 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);

7.21. 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).

7.22. O gestor do contrato deverá enviar a documentação pertinente ao setor de contratos para a formalização dos procedimentos de liquidação e pagamento, no valor dimensionado pela fiscalização e gestão nos termos do contrato.

8. CRITÉRIOS DE MEDIÇÃO E PAGAMENTO

8.1. Critérios de Aceitação

8.1.1. Os critérios de aceite da contratação serão baseados nos requisitos deste Termo de Referência, principalmente aqueles relativos à segurança, aos prazos de atendimento e à conformidade dos bens e serviços prestados;

8.1.2. Os equipamentos deverão ser novos e sem uso. Não serão aceitos equipamentos ou peças usadas, remanufaturadas ou de demonstração. Os equipamentos e peças deverão ser entregues nas caixas lacradas pelo fabricante. Não serão aceitos equipamentos e peças acondicionados em caixas violadas;

8.1.3. Todos os materiais referenciados nesta contratação deverão estar acondicionados e embalados conforme praxe do fabricante, protegendo o produto durante o transporte e armazenamento, com indicação do material contido, volume, data de fabricação, fabricante, importador, procedência, bem como demais informações exigidas na legislação em vigor;

8.1.4. A CONTRATANTE poderá efetuar consulta do número de série do equipamento, junto ao fabricante, informando data de compra e empresa adquirente, confirmando a procedência legal dos equipamentos;

8.1.5. A CONTRATANTE também poderá efetuar consulta junto aos órgãos competentes para certificar a legalidade do processo de importação, quando e se aplicável;

8.1.6. A UFPR se reserva o direito de rejeitar no todo ou em parte os bens ou serviços objeto da ARP, se considerar em desacordo com o estabelecido no presente Termo de Referência;

8.1.7. Todos os custos decorrentes da entrega ou substituição (transporte, documentação, conserto, hospedagem, alimentícios, etc.) correrão por conta da CONTRATADA.

8.2. Níveis Mínimos de Serviço Exigidos

8.2.1. Os níveis mínimos de serviço são indicadores mensuráveis estabelecidos pela Contratante para aferir objetivamente os resultados pretendidos com a contratação. Os níveis mínimos de serviço esperados, bem como para os atendimentos aos eventos associados a incidentes, problemas e ocorrências

relativas ao objeto da contratação, devem atender as condições estabelecidas pelo fabricante Fortinet para o serviço **FortiCare PREMIUM**, disponível em: <<https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-technical-support-and-rma-services.pdf>>.

8.2.2. Deverá ser disponibilizada, cumulativamente, sem ônus adicional para a CONTRATANTE, as seguintes formas de registro das demandas para suporte, em língua portuguesa:

- i. Estrutura de suporte técnico via atendimento telefônico e, opcionalmente, também por meio de chat no site do fabricante e;
- ii. Sistema web de *help-desk* (sistema de chamados) e, opcionalmente, também via e-mail. No caso de solicitações abertas via e-mail, a demanda deverá ser registrada no sistema de chamados para acompanhamento da solicitação.

8.2.3. Independentemente da forma utilizada para abertura do chamado, o número de atendimentos para os itens contratados deverá ser ilimitado, dentro do período de garantia.

8.2.4. Os atendimentos *on-site* na UFPR serão realizados no intervalo das 08:00 às 18:00 horas (horário de Brasília), de segunda a sexta-feira, exceto em finais de semana e em feriados nacionais ou dos municípios em que ocorrer o atendimento. Eventualmente, a CONTRATANTE e a CONTRATADA podem estabelecer horários diferenciados de acordo com a necessidade e conveniência, sem ônus adicional à UFPR.

8.2.5. Além do atendimento *on-site*, serão permitidos atendimentos remotos para identificação e solução de problemas, seguindo as seguintes premissas:

- i. A CONTRATADA deve informar antecipadamente à CONTRATANTE qualquer necessidade de acesso remoto;
- ii. O acesso remoto será controlado pela CONTRATANTE e só poderá ser habilitado com autorização expressa da CONTRATANTE;
- iii. Todas as intervenções realizadas remotamente são de responsabilidade da CONTRATADA, cabendo à mesma responder por quaisquer danos decorrentes dessas intervenções.

8.2.6. A CONTRATADA não será penalizada por atrasos nos prazos quando evidenciado o atraso por culpa da CONTRATANTE, portanto desconsiderar-se-á, para efeitos de cálculo dos prazos, os problemas decorrentes de falhas na infraestrutura elétrica ou na rede de dados da UFPR, como em geradores, nobreaks, switches, cabos, ataques à rede ou em decorrência de qualquer eventualidade que ocorra por motivo de força maior, imprevisível ou de difícil previsão, alheia à vontade de ambas as partes, que não permita acesso ao ambiente da Solução de Tecnologia da Informação, diagnóstico ou resolução do problema e que não tenham sido provocadas por falhas decorrentes dos mesmos. De qualquer forma, a CONTRATADA se obriga a notificar a CONTRATANTE, requerendo extensões de prazo e justificando claramente os motivos, que serão alvo de avaliação pela UFPR antes de recusa ou aceitação.

8.3. Do recebimento

8.3.1. 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.

8.3.2. No ato da entrega, a CONTRATADA deverá comprovar a aquisição de Garantia junto ao fabricante para os equipamentos e softwares relacionados na nota fiscal ou instrumento de cobrança equivalente.

8.3.3. Os bens e serviços 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 conforme prazos estabelecidos na Tabela 6 – Prazos de Entrega, a contar da notificação da CONTRATADA, às suas custas, sem prejuízo da aplicação das penalidades.

8.3.4. O recebimento definitivo ocorrerá no prazo de até 30 (trinta) dias corridos a partir do recebimento provisório, 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.

8.3.5. 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.

8.3.6. O prazo para a solução, pela CONTRATADA, 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.

8.3.7. O recebimento provisório ou definitivo não excluirá a responsabilidade civil pela solidez e pela segurança dos bens nem a responsabilidade ético-profissional pela perfeita execução do contrato.

8.4. Procedimentos de Teste e Inspeção

8.4.1. Serão adotados como procedimentos de teste e inspeção:

- a) Os resultados alcançados em relação à CONTRATADA, com a verificação dos prazos de execução e da qualidade demandada;
- b) A qualidade e quantidade dos recursos fornecidos;
- c) A adequação dos serviços prestados à rotina de execução estabelecida;
- d) O cumprimento das demais obrigações decorrentes do Contrato.

8.4.2. Poderão ser empregados pela equipe de fiscalização, a critério da UFPR:

- a) Mecanismos de controle, inspeção e avaliação da Solução de TIC;
- b) Indicadores para medição da conformidade (avaliação da qualidade e da adequação da solução de TIC);
- c) Origem e formas de obtenção das informações necessárias à gestão e à fiscalização do objeto, conforme Instrução Normativa SGD/ME nº 94/2022;
- d) Ferramentas a serem utilizadas para implantação e acompanhamento dos indicadores de conformidade;
- e) Listas de Verificação e Roteiro de Testes para subsidiar a ação dos Fiscais do Contrato;
- f) Garantia de diligências, quando aplicáveis, e suas formas de exercício.

8.4.3. A verificação da qualidade e adequação da solução de TIC será realizada com base nos critérios previstos neste Termo de Referência e seus anexos;

8.4.4. A fiscalização e o acompanhamento, com vistas à perfeita execução do objeto pela UFPR, não desobriga a CONTRATADA da mesma responsabilidade, com seus recursos próprios, garantidos os métodos, metodologias e ferramentas que julgar necessário a CONTRATADA.

8.5. Sanções Administrativas e Procedimentos para retenção ou glosa no pagamento

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

- a) der causa à inexecução parcial do contrato;
- b) der causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo;
- c) der causa à inexecução total do contrato;
- d) ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado;
- e) apresentar documentação falsa ou prestar declaração falsa durante a execução do contrato;
- f) praticar ato fraudulento na execução do contrato;
- g) comportar-se de modo inidôneo ou cometer fraude de qualquer natureza;
- h) praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013.

8.5.2. Serão aplicadas à CONTRATADA que incorrer nas infrações acima descritas as seguintes sanções:

- i. **Advertência**, quando a CONTRATADA der causa à inexecução parcial do contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, §2º, da Lei nº 14.133, de 2021);
- ii. **Impedimento de licitar e contratar**, quando praticadas as condutas descritas nas alíneas “b”, “c” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);
- iii. **Declaração de inidoneidade para licitar e contratar**, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).
- iv. **Multa**, considerando os seguintes parâmetros:

Tabela 9 – Infrações e Sanções Administrativas

Falha apurada	Fundamento legal	Sanção	Multa
Dar causa à inexecução parcial do contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do valor do empenho.
Deixar de prestar garantia ou assistência técnica aos materiais fornecidos	Lei 14.133/2021, art. 155 inc. I	Advertência	De 0,5 a 20% do valor do empenho.
Recusar-se ou deixar de prestar parcela do Contrato de fornecimento ou de prestação dos serviços, nos prazos contratados	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho.
Interromper a prestação dos serviços ou o fornecimento continuado, após iniciada a execução do Contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	Até 10% do valor total remanescente da obrigação.
Recusar-se ou deixar de atender solicitação formal da fiscalização do Contrato, necessários à boa execução contratual	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho.
Recusar-se ou deixar de cumprir normas internas da UFPR, apontadas em relatório de fiscalização	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho.
Deixar de ressarcir danos ao patrimônio da UFPR ou à integridade física ou patrimonial de terceiros, em decorrência de ação ou omissão durante a execução do Contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	Moratória de 0,2% por dia em que a falha persistir. Compensatória de até 10% do valor do empenho, sem prejuízo das demais custas com o ressarcimento dos danos causados
Entregar material ou serviço com características diversas daquelas constantes no Edital de Licitação, recusando-se ou deixando de efetuar a substituição no prazo fixado pela UFPR	Lei 14.133/2021, art. 155 inc. I	Advertência	Até 10% em relação ao valor da obrigação.
Entregar material ou serviço com características diversas daquelas constantes no Edital de Licitação, efetuando a substituição fora do prazo fixado pela UFPR	Lei 14.133/2021, art. 155 inc. I	Advertência	Moratória de 0,5% por dia de atraso. Compensatória de até 5% em relação ao valor da obrigação.

Dar causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo	Lei 14.133/2021, art. 155 inc. II	Impedimento de licitar e contratar no âmbito da União por até 1 ano	Agravada em 50% em relação à prevista para os casos de advertência.
Dar causa à inexecução total do contrato	Lei 14.133/2021, art. 155 inc. III	Impedimento de licitar e contratar no âmbito da União por até 3 anos	Até 30% em relação ao valor total da ARP
Recusar-se ou deixar de fornecer material ou serviço registrado em Ata de registro de preços	Lei 14.133/2021, art. 155 inc. III	Impedimento de licitar e contratar no âmbito da União por até 3 anos	Até 30% em relação ao valor total da ARP.
Recusar-se ou deixar de fornecer os materiais ou de prestar os serviços, integralmente	Lei 14.133/2021, art. 155 inc. III	Impedimento de licitar e contratar no âmbito da União por até 3 anos	Até 30% em relação ao valor total da ARP.
Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Até 10% em relação ao valor total da ARP.
Atrasar a entrega de material por prazo de até 30 dias.	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Moratória de 0,3% por dia de atraso.
Atrasar a entrega de material por prazo superior a 30 (trinta) dias.	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Moratória de 0,5% por dia de atraso. Compensatória de até 5% em relação ao valor da obrigação.
Prestar declaração falsa durante a execução do contrato	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Fazer declaração falsa sobre seu enquadramento fiscal	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Praticar ato fraudulento na execução do contrato	Lei 14.133/2021, art. 155 inc. IX	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.

Comportar-se de modo inidôneo	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Cometer fraude de qualquer natureza	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Omitir informações em notas fiscais	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Falsificar ou alterar notas fiscais	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.
Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013	Lei 14.133/2021, art. 155 inc. XII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total da ARP.

8.5.3. As sanções listadas na tabela acima não esgotam a possibilidade de enquadramento das condutas da CONTRATADA nas infrações previstas nesta Seção, com a aplicação das penalidades cabíveis.

8.5.4. A aplicação das sanções previstas neste Contrato não exclui, em hipótese alguma, a obrigação de reparação integral do dano causado à Contratante (art. 156, §9º, da Lei nº 14.133, de 2021).

8.5.5. Todas as sanções previstas neste Contrato poderão ser aplicadas cumulativamente com a multa (art. 156, §7º, da Lei nº 14.133, de 2021).

- 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 pela CONTRATANTE à CONTRATADA, 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.

8.5.6. A aplicação das sanções realizar-se-á em processo administrativo que assegure o contraditório e a ampla defesa à CONTRATADA, 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.

8.5.7. 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 a Contratante;
- e) a implantação ou o aperfeiçoamento de programa de integridade, conforme normas e orientações dos órgãos de controle.

8.5.8. 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).

8.5.9. A personalidade jurídica da CONTRATADA 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 a CONTRATADA, 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).

8.5.10. A Contratante deverá, no prazo máximo 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).

8.5.11. 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.

8.5.12. Os débitos da CONTRATADA 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 a CONTRATADA possua com o mesmo órgão ora Contratante, na forma da Instrução Normativa SEGES/ME nº 26, de 13 de abril de 2022.

8.6. Liquidação

8.6.1. Recebida a Nota Fiscal ou documento de cobrança equivalente, correrá o prazo de 10 (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.

8.6.2. 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.

8.6.3. 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:

- a) o prazo de validade;
- b) a data da emissão;
- c) os dados do contrato e do órgão Contratante;
- d) o período respectivo de execução do contrato;
- e) o valor a pagar; e
- f) eventual destaque do valor de retenções tributárias cabíveis.

8.6.4. 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 a Contratada providencie as medidas saneadoras, reiniciando-se o prazo após a comprovação da regularização da situação, sem ônus à Contratante.

8.6.5. 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.

8.6.6. 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).

8.6.7. Constatando-se, junto ao SICAF, a situação de irregularidade da Contratada, 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 da Contratante.

8.6.8. Não havendo regularização ou sendo a defesa considerada improcedente, a Contratante deverá comunicar aos órgãos responsáveis pela fiscalização da regularidade fiscal quanto à inadimplência da Contratada, 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.

8.6.9. Persistindo a irregularidade, a Contratante deverá adotar as medidas necessárias à rescisão contratual nos autos do processo administrativo correspondente, assegurada à Contratada a ampla defesa.

8.6.10. Havendo a efetiva execução do objeto, os pagamentos serão realizados normalmente, até que se decida pela rescisão do contrato, caso a Contratada não regularize sua situação junto ao SICAF.

8.7. Prazo de pagamento

8.7.1. 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.

8.7.2. No caso de atraso pela CONTRATANTE, os valores devidos à CONTRATADA serão atualizados monetariamente entre o termo final do prazo de pagamento até a data de sua efetiva realização, mediante aplicação do Índice Nacional de Preços ao Consumidor Amplo – IPCA de correção monetária.

8.8. Forma de pagamento

8.8.1. O pagamento será realizado por meio de ordem bancária, para crédito em banco, agência e conta corrente indicados pela Contratada.

8.8.2. Será considerada data do pagamento o dia em que constar como emitida a ordem bancária para pagamento.

8.8.3. Quando do pagamento, será efetuada a retenção tributária prevista na legislação aplicável.

8.8.4. Independentemente do percentual de tributo informado em sua proposta, quando houver, serão retidos na fonte, quando da realização do pagamento, os percentuais estabelecidos na legislação vigente.

8.8.5. A Contratada 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.

8.9. Cessão de crédito

8.9.1. 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.

8.9.2. A eficácia da cessão de crédito, de qualquer natureza, em relação à Administração, está condicionada à celebração de termo aditivo ao contrato administrativo.

8.9.3. Sem prejuízo do regular atendimento da obrigação contratual de cumprimento de todas as condições de habilitação por parte da Contratada (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.

8.9.4. O crédito a ser pago à cessionária é exatamente aquele que seria destinado à cedente (Contratada) 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.

8.9.5. A cessão de crédito não afetará a execução do objeto contratado, que continuará sob a integral responsabilidade da Contratada.

9. FORMA E CRITÉRIOS DE SELEÇÃO DO FORNECEDOR

9.1. Forma de seleção e critério de julgamento da proposta

9.1.1. 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.

9.1.2. O modo de disputa será o Aberto, tendo como intervalo de lances em 0,25% do valor dos itens convertidos em moeda Real.

9.2. Da Aplicação da Margem de Preferência

9.2.1. Não será aplicada margem de preferência na presente contratação, em atenção à Resolução SEGES/CICS/MGI nº 06/2024, a qual suspende a aplicação de margens de preferência em licitações que tenham por critério de julgamento o menor preço por grupo de itens.

9.3. Cotas para ME/EPP

9.3.1. O art. 10 do Decreto 8.538/2015 estabelece que não se aplica o disposto nos art. 6º ao art. 8º quando, o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte, não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou ao complexo do objeto a ser contratado, justificadamente. Conforme avaliação do Estudo Técnico Preliminar, os itens da presente contratação serão disputados pela ampla concorrência, visando maior competitividade e preços mais vantajosos para a Administração Pública, bem como a redução do risco de fracasso em alguns itens do processo licitatório.

9.4. Exigências de habilitação

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

9.4.1.1. Habilitação jurídica

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

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

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

d) No caso de 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 nº 77, de 18 de março de 2020.

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

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

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

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

9.4.1.2. Habilitação fiscal, social e trabalhista

9.4.1.2.1. Prova de inscrição no Cadastro Nacional de Pessoas Jurídicas ou no Cadastro de Pessoas Físicas, conforme o caso;

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

9.4.1.2.3. Prova de regularidade com o Fundo de Garantia do Tempo de Serviço (FGTS);

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

9.4.1.2.5. Prova de inscrição no cadastro de contribuintes Estadual relativo ao domicílio ou sede do fornecedor, pertinente ao seu ramo de atividade e compatível com o objeto contratual;

9.4.1.2.6. Prova de regularidade com a Fazenda Estadual do domicílio ou sede do fornecedor, relativa à atividade em cujo exercício contrata ou concorre;

9.4.1.2.7. Caso o fornecedor seja considerado isento dos tributos Estaduais 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;

9.4.1.2.8. O fornecedor enquadrado como microempreendedor individual que pretenda auferir os benefícios do tratamento diferenciado previstos na Lei Complementar nº 123, de 2006, estará dispensado da prova de inscrição nos cadastros de contribuintes estadual e municipal.

9.4.1.3. Qualificação Econômico-Financeira

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

9.4.1.4. Qualificação Técnica

9.4.1.4.1. **Declaração que ateste a inexistência da prática de “registro de oportunidade”** (conforme Anexo E). Essa declaração tem por objetivo garantir o princípio constitucional da isonomia e da seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 14.133, de 2021.

9.4.1.4.2. **Certidão ou Atestado de Capacidade Técnica emitido por pessoa jurídica de direito público ou privado**, comprovando que a proponente fornece ou forneceu firewalls compatíveis com os itens 1, 3 ou 5. Também deverá ser apresentado documento comprovando que a proponente fornece ou forneceu pontos de acesso compatíveis com os itens 7, 8 e 9.

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

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

lii. 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.

9.5. Dos Documentos para Aferição da Proposta

9.5.1. A análise técnica das propostas será realizada exclusivamente a partir dos catálogos, fichas técnicas, declarações, atestados e certificados dos produtos ofertados apresentados pela licitante juntamente com sua proposta.

9.5.2. Para aferição das propostas as licitantes deverão anexar no sistema Comprasnet, em até 24 (vinte e quatro) horas a partir da solicitação da Pregoeira, os seguintes documentos, sob pena de desclassificação:

a) Declaração de que todos os produtos são novos e de primeiro uso. Não serão aceitos equipamentos e peças usadas, remanufaturadas, de demonstração ou acondicionados em caixas violadas.

b) Catálogos e/ou fichas técnicas do fabricante ou, ainda, indicar endereço eletrônico do fabricante, no qual se possa comparar o produto ofertado com a especificação solicitada neste Termo de Referência e verificar as demais características do mesmo. A documentação é obrigatória para os itens 1, 3, 5, 7, 8, 9, 10, 11, 14, 17, 19, 21, 23, 24, 26, 28, 30, 31, 32 e 33 da presente contratação.

c) Comprovante de que a empresa está relacionada como *partner*, caso não seja ela própria o fabricante, atestando que a CONTRATADA é a representante autorizada, e está habilitada a comercializar, prestar serviços de instalação, configuração e suporte técnico aos equipamentos e softwares do fabricante, sem prejuízo da garantia. Essa exigência pode ser comprovada das seguintes formas:

i. indicação da página na Internet (URL do *website*) do fabricante que contenha esta informação; ou

ii. cópia do contrato entre a licitante e o fabricante; ou

iii. declaração do fabricante informando que a licitante é revendedora ou distribuidora autorizada.

9.6. No caso de Participação de Cooperativas

9.6.1. No caso da participação de cooperativas, será exigida a seguinte documentação complementar:

9.6.1.1. A relação dos cooperados que atendem aos requisitos técnicos exigidos para a contratação e que executarão o contrato, com as respectivas atas de inscrição e a comprovação de que estão domiciliados na localidade da sede da cooperativa, respeitado o disposto nos arts. 4º, inciso XI, 21, inciso I e 42, §§2º a 6º da Lei n. 5.764, de 1971;

9.6.1.2. A declaração de regularidade de situação do contribuinte individual – DRSCI, para cada um dos cooperados indicados;

9.6.1.3. A comprovação do capital social proporcional ao número de cooperados necessários à prestação do serviço;

9.6.1.4. O registro previsto na Lei n. 5.764, de 1971, art. 107;

9.6.1.5. A comprovação de integração das respectivas quotas-partes por parte dos cooperados que executarão o contrato;

9.6.1.6. Os seguintes documentos para a comprovação da regularidade jurídica da cooperativa: a) ata de fundação; b) estatuto social com a ata da assembleia que o aprovou; c) regimento dos fundos instituídos pelos cooperados, com a ata da assembleia; d) editais de convocação das três últimas assembleias gerais extraordinárias; e) três registros de presença dos cooperados que executarão o contrato em assembleias gerais ou nas reuniões seccionais; e f) ata da sessão que os cooperados autorizaram a cooperativa a contratar o objeto da licitação; e

9.6.1.7. A última auditoria contábil-financeira da cooperativa, conforme dispõe o art. 112 da Lei n. 5.764, de 1971, ou uma declaração, sob as penas da lei, de que tal auditoria não foi exigida pelo órgão fiscalizador.

9.7. No caso de participação de Consórcio

9.7.1. No caso da participação de Consórcio, será exigida a seguinte documentação complementar:

9.7.1.1. Comprovação de compromisso público ou particular de constituição de consórcio, subscrito pelos consorciados;

9.7.1.2. Indicação da empresa líder do consórcio, que será responsável por sua representação perante a Administração;

9.7.1.3. Admissão, para efeito de habilitação técnica, do somatório dos quantitativos de cada consorciado e, para efeito de habilitação econômico-financeira, do somatório dos valores de cada consorciado;

9.7.1.4. Não será permitida a participação de empresas consorciadas, na mesma licitação, de mais de um consórcio ou de forma isolada.

9.8. Dos documentos necessários para assinatura da Ata de Registro de Preços

9.8.1. Recomenda-se que os licitantes providenciem seu cadastro no sistema de processo eletrônico da UFPR, visando agilizar os trâmites para assinatura da ata de registro de preços (Anexo III do edital de licitação).

9.8.1.1. O cadastro deve ser feito pelo representante legal da empresa, no sítio www.sei.ufpr.br/sei, escolhendo a opção "Acesso Usuário Externo".

9.8.1.2. A assinatura da ata de registro de preços (Anexo III do edital de licitação) poderá ser realizada através do Sistema de Processo Eletrônico da UFPR.

9.8.1.2.1. Não haverá envio de documentos por correio nas situações cuja assinatura da ata de registro de preços (Anexo III do edital de licitação) seja realizada através do Sistema de Processo Eletrônico da UFPR.

9.8.2. Para a assinatura da Ata de Registro de Preços a licitante vencedora deverá apresentar os seguintes documentos:

a) Termo de Compromisso e Manutenção de Sigilo assinado, conforme Anexo C desse Termo de Referência;

b) Declaração de Garantia: para os itens 1, 3, 5, 7, 8, 9, 10, 30, 31, 32 e 33, a CONTRATADA deverá declarar aquisição da garantia junto ao fabricante para assegurar que os equipamentos e peças estejam certificados e em conformidade com a política de garantia do fabricante. Deverá ainda indicar na proposta final o SKU ou *part number* dos equipamentos, conforme Anexo F – DECLARAÇÃO DE GARANTIA;

10. ESTIMATIVAS DO VALOR DA CONTRATAÇÃO

10.1. O custo estimado total da contratação é de **R\$ 11.974.559,57 (onze milhões novecentos e setenta e quatro mil quinhentos e cinquenta e nove reais e cinquenta e sete centavos)**, conforme custos unitários e totais apresentados na seção "CONDIÇÕES GERAIS DA CONTRATAÇÃO".

10.2. 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;

10.2.3. 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;

10.2.4. Serão reajustados os preços registrados, respeitada a contagem da anualidade com aplicação do Índice de Custo da Tecnologia da Informação (ICTI) para a contratação; ou

10.2.5. Poderão ser repactuados, a pedido do interessado, conforme critérios definidos para a contratação.

11. ADEQUAÇÃO ORÇAMENTÁRIA

11.1. Não se aplica a informação de dotação orçamentária prévia à presente contratação, por se tratar de formação de registro de preços. A indicação da disponibilidade de créditos orçamentários somente será exigida para a formalização do Contrato, nos termos do art. 17 do Decreto 11.462/2023.

12. DOS CASOS OMISSOS

12.1. 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.

13. DA EQUIPE DE PLANEJAMENTO DA CONTRATAÇÃO E DA APROVAÇÃO

13.1. A Equipe de Planejamento da Contratação foi instituída pela Portaria Interna 227/2024-CLIC ([7167384](#)), de 16 de outubro de 2024.

13.2. Conforme o §6º do art. 12 da IN SGD/ME nº 94/2022, o Termo de Referência será assinado pela Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC e aprovado pela autoridade competente.

Integrante Requisitante	Integrantes Técnicos	Integrantes Administrativos
Gustavo de Brito dos Santos Coordenador da Coordenação de Serviços e Infraestrutura de TIC (CSI) Matrícula/SIAPE: 1111747	Giovanni Allam Taborda Analista de Tecnologia da Informação Matrícula/SIAPE: 2909475 Valmir Antunes Pereira Gestor de Segurança da Informação Matrícula/SIAPE: 1526015	Edivan Bubinski Linhares Assistente em Administração Matrícula/SIAPE: 2964044 Franciane Aparecida Cavalin Administrador Matrícula/SIAPE: 1115106

Autoridade Máxima da Área de TIC
Felipe Sanches Bueno Diretor Executivo da AGTIC Matrícula/SIAPE: 1653832

ANEXO A - ESPECIFICAÇÕES TÉCNICAS DOS ITENS

ITEM 1 - SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses

- Throughput de, no mínimo, 197 Gbps com a funcionalidade de firewall habilitada para pacotes de 512bytes.
- Suporte a, no mínimo, 12.000.000 conexões simultâneas;
- Suporte a, no mínimo, 750 mil novas conexões por segundo;
- Throughput de, no mínimo, 55 Gbps de VPN IPSec, com pacotes de no mínimo 512 bytes;
- Estar licenciado para, ou suportar sem o uso de licença, 20.000 túneis de VPN IPSEC Site-to-Site simultâneos;
- Suportar no mínimo 22 Gbps de throughput de IPS;
- Suporte a, no mínimo, 34 Gbps de throughput de Application Control;
- Suportar no mínimo 12 Gbps de throughput de Inspeção SSL;
- Possuir ao menos 4 interfaces 100 GE QSFP28/40 GE QSFP+ Slots;
- Possuir ao menos 12 interfaces 25 GE SFP28/10 GE SFP+/GE SFP Slots;
- Possuir ao menos 8 interfaces GE SFP;
- 16 interfaces GE RJ45;
- Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por equipamento, com garantia de 60 meses on-site.

Características gerais:

- A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, não sendo permitidos appliances virtuais ou solução open source (produto montado);
- Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
- Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;
- As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;
- A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
- Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 2U cada;
- O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;0
- Os dispositivos de proteção de rede devem possuir suporte a Vlans;
- Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
- Deve suportar BGP, OSPF, RIP e roteamento estático;
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
- Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
- Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
- Deve suportar NAT dinâmico (Many-to-Many);
- Deve suportar NAT estático (1-to-1);
- Deve suportar NAT estático bidirecional 1-to-1;
- Deve suportar Tradução de porta (PAT);
- Deve suportar NAT de Origem;
- Deve suportar NAT de Destino;

33. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
34. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
35. Deve suportar NAT64;
36. Deve implementar o protocolo ECMP;
37. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
38. Enviar log para sistemas de monitoração externos;
39. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
40. Proteção anti-spoofing;
41. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
42. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
43. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
44. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
45. A configuração em alta disponibilidade deve sincronizar: Sessões;
46. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QoS e objetos de rede;
47. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
48. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
49. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
50. Deve possuir suporte à criação de sistemas virtuais (VDMs) no mesmo appliance;
51. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
52. Controle, inspeção e descryptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
53. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
54. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

Políticas:

55. Deverá suportar controles por zonas de segurança;
56. Deverá suportar controles de políticas por porta e protocolo;
57. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
58. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
59. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
60. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
61. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2;
62. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
63. Suporte a objetos e regras IPV6;
64. Suporte a objetos e regras multicast;
65. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Aplicações:

66. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
67. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
68. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
69. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
70. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
71. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
72. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
73. Deve suportar a descryptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica;
74. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
75. Identificar o uso de táticas evasivas via comunicações criptografadas;
76. Atualizar a base de assinaturas de aplicações automaticamente;
77. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
78. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
79. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
80. 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;
81. Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação.
82. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
83. Deve alertar o usuário quando uma aplicação for bloqueada;
84. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
85. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
86. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
87. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
88. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);

89. 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;

90. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

Prevenção de ameaças:

91. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;

92. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);

93. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;

94. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e manter em quarentena o IP do atacante por um intervalo de tempo;

95. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;

96. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE assim como um "wildcard" do CVE para abranger mais de um identificador.

97. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;

98. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;

99. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;

100. Deve permitir o bloqueio de vulnerabilidades;

101. Deve permitir o bloqueio de exploits conhecidos;

102. Deve incluir proteção contra ataques de negação de serviços;

103. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;

104. Detectar e bloquear a origem de portscans;

105. Bloquear ataques efetuados por worms conhecidos;

106. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;

107. Possuir assinaturas para bloqueio de ataques de buffer overflow;

108. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;

109. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;

110. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;

111. Identificar e bloquear comunicação com botnets;

112. Registrar na console de monitoração 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;

113. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;

114. Os eventos devem identificar o país de onde partiu a ameaça;

115. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

116. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

117. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

118. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

119. A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;

120. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

121. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

122. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

Filtro de URLs:

123. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

124. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

125. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

126. 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;

127. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

128. Possuir pelo menos 60 categorias de URLs;

129. Deve possuir a função de exclusão de URLs do bloqueio;

130. Permitir a customização de página de bloqueio.

Identificação de usuários:

131. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

132. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

133. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server;

134. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

135. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

136. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

137. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída à internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

138. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

139. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

Filtro de dados:

- 140. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
- 141. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 142. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
- 143. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização:

- 144. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
- 145. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

VPN:

- 146. Suportar VPN Site-to-Site e Cliente-To-Site;
- 147. Suportar IPSec VPN;
- 148. Suportar SSL VPN;
- 149. A VPN IPSec deve suportar 3DES;
- 150. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;
- 151. A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
- 152. A VPN IPSec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
- 153. A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
- 154. A VPN IPSec deve suportar Autenticação via certificado IKE PKI;
- 155. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
- 156. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;
- 157. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;
- 158. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
- 159. Atribuição de DNS nos clientes remotos de VPN;
- 160. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;
- 161. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
- 162. Suportar leitura e verificação de CRL (certificate revocation list);
- 163. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulem dentro dos túneis SSL;
- 164. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
- 165. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
- 166. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
- 167. Deverá manter uma conexão segura com o portal durante a sessão;
- 168. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows, MacOS e Linux.

SD-WAN:

- 169. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
- 170. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo e twamp;
- 171. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
- 172. Deve suportar o uso de VRF (Virtual Routing and Forwarding);
- 173. A solução deve permitir a definição do roteamento para cada aplicação;
- 174. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
- 175. Deve possibilitar a definição do link de saída para uma aplicação específica;
- 176. Deve implementar balanceamento de link por hash do IP de origem;
- 177. Deve implementar balanceamento de link por hash do IP de origem e destino;
- 178. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;
- 179. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
- 180. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;
- 181. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);
- 182. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
- 183. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
- 184. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
- 185. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
- 186. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
- 187. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
- 188. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
- 189. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações;
- 190. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
- 191. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
- 192. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
- 193. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
- 194. O QoS deve possibilitar a definição de fila de prioridade;
- 195. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;

196. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
197. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;
198. Deve possibilitar a definição de bandas distintas para download e upload;
199. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
200. A solução de SD-WAN deve suportar IPv6;
201. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
202. Deve ser capaz de bloquear acesso a aplicações;
203. Deve suportar NAT dinâmico bem como NAT de saída;
204. Deve suportar balanceamento de tráfego por sessão e pacote;
205. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;
206. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
207. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
208. Deve implementar balanceamento de link por custo configurado do link;
209. Deve suportar o balanceamento de, no mínimo, 5 links;
210. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPsec;
211. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;
212. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
213. Deve suportar Zero-Touch Provisioning;
214. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
215. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
216. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
217. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
218. Suportar UDP Hole Punching em arquitetura ADVPN;
219. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
220. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
221. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
222. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;
223. Deve ser possível utilizar o balanceamento round Robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;
224. Deve ser possível especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida.

ITEM 2 - SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO I

1. O serviço corresponde ao item 1.
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço de configuração será fornecido para a implantação do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implantação

- 3.1.1. 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.

3.2. Cronograma do plano de implementação

- 3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

- 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

- 3.4.1. 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.
- 3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

- 3.5.1. 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.
4. 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;
5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;
6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;
7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados;
8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
9. 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;

10. 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;

11. 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.

ITEM 3 - SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses

1. Throughput de, no mínimo, 137.5 Gbps com a funcionalidade de firewall habilitada para pacotes de 512bytes;
2. Suporte a, no mínimo, 8.000.000 conexões simultâneas;
3. Suporte a, no mínimo, 550 mil novas conexões por segundo;
4. Throughput de, no mínimo, 55 Gbps de VPN IPSec, com pacotes de no mínimo 512 bytes;
5. Estar licenciado para, ou suportar sem o uso de licença, 2000 túneis de VPN IPSEC Site-to-Site simultâneos;
6. Suportar no mínimo 14 Gbps de throughput de IPS;
7. Suporte a, no mínimo, 32 Gbps de throughput de Application Control;
8. Suportar no mínimo 9 Gbps de throughput de Inspeção SSL;
9. Possuir ao menos 4 interfaces 25GE/10GE SFP28/SPF+, 4 interfaces 10GE SFP+, 8 interfaces GE SFP e 16 interfaces GE RJ45;
10. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por equipamento, com garantia de 60 meses on-site.

Características gerais:

11. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, não sendo permitidos appliances virtuais ou solução open source (produto montado);
12. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
13. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;
14. As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;
15. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
16. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;
17. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
18. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
19. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
20. Deve suportar BGP, OSPF, RIP e roteamento estático;
21. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
22. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
23. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
24. Deve suportar NAT dinâmico (Many-to-Many);
25. Deve suportar NAT estático (1-to-1);
26. Deve suportar NAT estático bidirecional 1-to-1;
27. Deve suportar Tradução de porta (PAT);
28. Deve suportar NAT de Origem;
29. Deve suportar NAT de Destino;
30. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
31. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
32. Deve suportar NAT64;
33. Deve implementar o protocolo ECMP;
34. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
35. Enviar log para sistemas de monitoração externos;
36. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
37. Proteção anti-spoofing;
38. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
39. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
40. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
41. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
42. A configuração em alta disponibilidade deve sincronizar: Sessões;
43. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
44. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
45. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
46. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
47. Deve possuir suporte à criação de sistemas virtuais (VDMs) no mesmo appliance;
48. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
49. Controle, inspeção e descryptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
50. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
51. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

Políticas:

52. Deverá suportar controles por zonas de segurança;
53. Deverá suportar controles de políticas por porta e protocolo;
54. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
55. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
56. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);

57. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
58. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2;
59. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
60. Suporte a objetos e regras IPV6;
61. Suporte a objetos e regras multicast;
62. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Aplicações:

63. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
64. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
65. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
66. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
67. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
68. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
69. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
70. Deve suportar a descryptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica.
71. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
72. Identificar o uso de táticas evasivas via comunicações criptografadas;
73. Atualizar a base de assinaturas de aplicações automaticamente;
74. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
75. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;
76. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
77. 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;
78. Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação.
79. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
80. Deve alertar o usuário quando uma aplicação for bloqueada;
81. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
82. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
83. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
84. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
85. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
86. 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;
87. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

Prevenção de ameaças:

88. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
89. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
90. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
91. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e manter em quarentena o IP do atacante por um intervalo de tempo;
92. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
93. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE assim como um "wildcard" do CVE para abranger mais de um identificador;
94. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
95. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
96. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
97. Deve permitir o bloqueio de vulnerabilidades;
98. Deve permitir o bloqueio de exploits conhecidos;
99. Deve incluir proteção contra ataques de negação de serviços;
100. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
101. Detectar e bloquear a origem de portscans;
102. Bloquear ataques efetuados por worms conhecidos;
103. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
104. Possuir assinaturas para bloqueio de ataques de buffer overflow;
105. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
106. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
107. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
108. Identificar e bloquear comunicação com botnets;
109. Registrar na console de monitoração 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;
110. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de

botnets conhecidas;

111. Os eventos devem identificar o país de onde partiu a ameaça;

112. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;

113. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;

114. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;

115. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;

116. A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;

117. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;

118. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;

119. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

Filtro de URLs:

120. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);

121. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;

122. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;

123. 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;

124. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;

125. Possuir pelo menos 60 categorias de URLs;

126. Deve possuir a função de exclusão de URLs do bloqueio;

127. Permitir a customização de página de bloqueio.

Identificação de usuários:

128. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;

129. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

130. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2;

131. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;

132. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

133. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;

134. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);

135. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;

136. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

Filtro de dados:

137. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);

138. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

139. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;

140. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização:

141. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;

142. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

VPN:

143. Suportar VPN Site-to-Site e Cliente-To-Site;

144. Suportar IPSec VPN;

145. Suportar SSL VPN;

146. A VPN IPSec deve suportar 3DES;

147. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;

148. A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;

149. A VPN IPSec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);

150. A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);

151. A VPN IPSec deve suportar Autenticação via certificado IKE PKI;

152. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;

153. A VPN SSL deve suportar o usuário realizar a conexão por meio de cliente instalado no sistema operacional do equipamento ou por meio de interface WEB;

154. A funcionalidades de VPN SSL devem ser atendidas com ou sem o uso de agente;

155. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;

156. Atribuição de DNS nos clientes remotos de VPN;

157. Dever permitir criar políticas de controle de aplicações, IPS, Antivírus, Antipyyware e filtro de URL para tráfego dos clientes remotos conectados na VPN SSL;

158. Suportar autenticação via AD/LDAP, certificado e base de usuários local;

159. Suportar leitura e verificação de CRL (certificate revocation list);

160. Permitir a aplicação de políticas de segurança e visibilidade para as aplicações que circulam dentro dos túneis SSL;

161. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
162. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
163. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
164. Deverá manter uma conexão segura com o portal durante a sessão;
165. O agente de VPN SSL ou IPSEC client-to-site deve ser compatível com pelo menos: Windows, MacOS e Linux.

SD-WAN:

166. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
167. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo e twamp;
168. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
169. Deve suportar o uso de VRF (Virtual Routing and Forwarding);
170. A solução deve permitir a definição do roteamento para cada aplicação;
171. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
172. Deve possibilitar a definição do link de saída para uma aplicação específica;
173. Deve implementar balanceamento de link por hash do IP de origem;
174. Deve implementar balanceamento de link por hash do IP de origem e destino;
175. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;
176. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
177. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;
178. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);
179. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
180. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
181. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
182. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
183. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
184. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
185. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
186. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações;
187. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
188. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;
189. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
190. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
191. O QoS deve possibilitar a definição de fila de prioridade;
192. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
193. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
194. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;
195. Deve possibilitar a definição de bandas distintas para download e upload;
196. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
197. A solução de SD-WAN deve suportar IPv6;
198. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
199. Deve ser capaz de bloquear acesso a aplicações;
200. Deve suportar NAT dinâmico bem como NAT de saída;
201. Deve suportar balanceamento de tráfego por sessão e pacote;
202. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;
203. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
204. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
205. Deve implementar balanceamento de link por custo configurado do link.
206. Deve suportar o balanceamento de, no mínimo, 5 links;
207. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPsec;
208. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;
209. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
210. Deve suportar Zero-Touch Provisioning;
211. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
212. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
213. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
214. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
215. Suportar UDP Hole Punching em arquitetura ADVPN;
216. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
217. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
218. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
219. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;

220. Deve ser possível utilizar o balanceamento round Robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;
221. Deve ser possível especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida.

ITEM 4 - SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO II

1. O serviço corresponde ao item 3.
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço de configuração será fornecido para a implantação do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implantação

3.1.1. 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.

3.2. Cronograma do plano de implementação

3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

3.4.1. 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.

3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

3.5.1. 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.

4. 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;

5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;

6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;

7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados;

8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;

9. 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;

10. 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;

11. 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.

ITEM 5 - SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses

1. Throughput de, no mínimo, 28 Gbps com a funcionalidade de firewall habilitada para pacotes de 512bytes.
2. Suporte a, no mínimo, 3.000.000 conexões simultâneas;
3. Suporte a, no mínimo, 124 mil novas conexões por segundo;
4. Throughput de, no mínimo, 25 Gbps de VPN IPSec, com pacotes de no mínimo 512 bytes;
5. Estar licenciado para, ou suportar sem o uso de licença, 200 túneis de VPN IPSEC Site-to-Site simultâneos;
6. Suportar no mínimo 4.5 Gbps de throughput de IPS;
7. Suporte a, no mínimo, 6.7 Gbps de throughput de Application Control;
8. Suportar no mínimo 2.6 Gbps de throughput de Inspeção SSL;
9. Possuir ao menos 2 interfaces 10/5/2.5/GE RJ45 ou 10GE/GE SFP+ (Shared Media pairs);
10. Possuir ao menos 8 interfaces GE RJ45;
11. Estar licenciado e/ou ter incluído sem custo adicional, no mínimo, 10 sistemas virtuais lógicos (Contextos) por equipamento, com garantia de 60 meses on-site.

Características gerais:

12. A solução deve consistir em plataforma de proteção de rede baseada em appliance físico com funcionalidades de Next Generation Firewall (NGFW) e SD-WAN, não sendo permitidos appliances virtuais ou solução open source (produto montado);
13. Por funcionalidades de NGFW entende-se: reconhecimento de aplicações, prevenção de ameaças, identificação de usuários e controle granular de permissões;
14. Por funcionalidades de SD-WAN entende-se: roteamento inteligente, uso do melhor link por aplicação, abstração do tráfego em relação aos circuitos físicos e controle do tráfego por aplicação;
15. As funcionalidades de segurança e SD-WAN que compõem a solução podem funcionar em múltiplos appliances desde que obedeçam a todos os requisitos desta especificação, acompanhem os mesmos termos de garantia, atualizações e manutenção, e suportem gerenciamento centralizado;
16. A plataforma deve ser otimizada para análise de conteúdo de aplicações em camada 7;
17. Todos os equipamentos fornecidos não devem ultrapassar a medida máxima de 1U cada;

18. O gerenciamento da solução deve suportar acesso via SSH, cliente ou WEB (HTTPS) e API aberta;
19. Os dispositivos de proteção de rede devem possuir suporte a Vlans;
20. Os dispositivos de proteção de rede devem possuir suporte a roteamento multicast (PIM-SM e PIM-DM);
21. Deve suportar BGP, OSPF, RIP e roteamento estático;
22. Os dispositivos de proteção de rede devem possuir suporte a DHCP Relay;
23. Os dispositivos de proteção de rede devem possuir suporte a DHCP Server;
24. Os dispositivos de proteção de rede devem suportar sub-interfaces ethernet logicas;
25. Deve suportar NAT dinâmico (Many-to-Many);
26. Deve suportar NAT estático (1-to-1);
27. Deve suportar NAT estático bidirecional 1-to-1;
28. Deve suportar Tradução de porta (PAT);
29. Deve suportar NAT de Origem;
30. Deve suportar NAT de Destino;
31. Deve suportar NAT de Origem e NAT de Destino simultaneamente;
32. Deve implementar Network Prefix Translation (NPTv6) ou NAT66, prevenindo problemas de roteamento assimétrico;
33. Deve suportar NAT64;
34. Deve implementar o protocolo ECMP;
35. Deve permitir monitorar via SNMP o uso de CPU, memória, espaço em disco, VPN, situação do cluster e violações de segurança;
36. Enviar log para sistemas de monitoração externos;
37. Deve haver a opção de enviar logs para os sistemas de monitoração externos via protocolo SSL;
38. Proteção anti-spoofing;
39. Deve suportar Modo Sniffer, para inspeção via porta espelhada do tráfego de dados da rede;
40. Deve suportar Modo Camada – 2 (L2), para inspeção de dados em linha e visibilidade do tráfego;
41. Deve suportar Modo Camada – 3 (L3), para inspeção de dados em linha e visibilidade do tráfego;
42. Suporte a configuração de alta disponibilidade Ativo/Passivo e Ativo/Ativo: Em modo layer 3;
43. A configuração em alta disponibilidade deve sincronizar: Sessões;
44. A configuração em alta disponibilidade deve sincronizar: Configurações, incluindo, mas não limitado as políticas de Firewall, NAT, QOS e objetos de rede;
45. A configuração em alta disponibilidade deve sincronizar: Associações de Segurança das VPNs;
46. A configuração em alta disponibilidade deve sincronizar: Tabelas FIB;
47. O HA (modo de Alta-Disponibilidade) deve possibilitar monitoração de falha de link;
48. Deve possuir suporte à criação de sistemas virtuais (VDMs) no mesmo appliance;
49. Deve permitir a criação de administradores independentes, para cada um dos sistemas virtuais existentes, de maneira a possibilitar a criação de contextos virtuais que podem ser administrados por equipes distintas;
50. Controle, inspeção e descryptografia de SSL para tráfego de Saída (Outbound), devendo suportar o controle dos certificados individualmente dentro de cada sistema virtual, ou seja, isolamento das operações de adição, remoção e utilização dos certificados diretamente nos sistemas virtuais (contextos);
51. Não serão aceitas soluções baseadas em PCs de uso geral. Todos os equipamentos a serem fornecidos deverão ser do mesmo fabricante para assegurar a padronização e compatibilidade funcional de todos os recursos;
52. Os equipamentos devem ser novos, ou seja, de primeiro uso, de um mesmo fabricante. Na data da proposta, nenhum dos modelos ofertados poderão estar listados no site do fabricante em listas de end-of-life e end-of-sale.

Políticas:

53. Deverá suportar controles por zonas de segurança;
54. Deverá suportar controles de políticas por porta e protocolo;
55. Deverá suportar controles de políticas por aplicações, grupos estáticos de aplicações e grupos dinâmicos de aplicações;
56. Controle de políticas por usuários, grupos de usuários, IPs, redes e zonas de segurança;
57. Controle de políticas por código de País (Por exemplo: BR, US, UK, RU);
58. Controle, inspeção e descryptografia de SSL por política para tráfego de saída (Outbound);
59. Deve descryptografar tráfego outbound em conexões negociadas com TLS 1.2;
60. Deve permitir o bloqueio de arquivo por sua extensão e possibilitar a correta identificação do arquivo por seu tipo mesmo quando sua extensão for renomeada;
61. Suporte a objetos e regras IPV6;
62. Suporte a objetos e regras multicast;
63. Suportar a atribuição de agendamento das políticas com o objetivo de habilitar e desabilitar políticas em horários pré-definidos automaticamente.

Aplicações:

64. Os dispositivos de proteção de rede deverão possuir a capacidade de reconhecer aplicações, independente de porta e protocolo;
65. Deve ser possível a liberação e bloqueio somente de aplicações sem a necessidade de liberação de portas e protocolos;
66. Reconhecer pelo menos 1700 aplicações diferentes, incluindo, mas não limitado: a tráfego relacionado a peer-to-peer, redes sociais, acesso remoto, update de software, protocolos de rede, voip, áudio, vídeo, proxy, mensageiros instantâneos, compartilhamento de arquivos, e-mail;
67. Reconhecer pelo menos as seguintes aplicações: bittorrent, gnutella, skype, facebook, linked-in, twitter, citrix, logmein, teamviewer, ms-rdp, vnc, gmail, youtube, http-proxy, http-tunnel, facebook chat, gmail chat, whatsapp, 4shared, dropbox, google drive, skydrive, db2, mysql, oracle, active directory, kerberos, ldap, radius, itunes, dhcp, ftp, dns, wins, msrpc, ntp, snmp, rpc over http, gotomeeting, webex, evernote, google-docs;
68. Deve inspecionar o payload de pacote de dados com o objetivo de detectar assinaturas de aplicações conhecidas pelo fabricante independente de porta e protocolo;
69. Identificar o uso de táticas evasivas, ou seja, deve ter a capacidade de visualizar e controlar as aplicações e os ataques que utilizam táticas evasivas via comunicações criptografadas, tais como Skype e utilização da rede Tor;
70. Para tráfego criptografado SSL, deve descryptografar pacotes a fim de possibilitar a leitura de payload para checagem de assinaturas de aplicações conhecidas pelo fabricante;
71. Deve suportar a descryptografia do tráfego SSL (IPv4 e IPv6) e espelhar este tráfego para uma interface específica;
72. Deve realizar decodificação de protocolos com o objetivo de detectar aplicações encapsuladas dentro do protocolo e validar se o tráfego corresponde com a especificação do protocolo. A decodificação de protocolo também deve identificar funcionalidades específicas dentro de uma aplicação;
73. Identificar o uso de táticas evasivas via comunicações criptografadas;
74. Atualizar a base de assinaturas de aplicações automaticamente;
75. Os dispositivos de proteção de rede devem possuir a capacidade de identificar o usuário de rede com integração ao Microsoft Active Directory, sem a necessidade de instalação de agente no Domain Controller, nem nas estações dos usuários;
76. Deve ser possível adicionar controle de aplicações em múltiplas regras de segurança do dispositivo, ou seja, não se limitando somente a possibilidade de habilitar controle de aplicações em algumas regras;

77. Deve suportar vários métodos de identificação e classificação das aplicações, por pelo menos checagem de assinaturas e decodificação de protocolos;
78. 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;
79. Deve permitir exceções de aplicações caso uma regra de controle de aplicação seja configurada para permitir ou bloquear uma categoria de aplicação;
80. O fabricante deve permitir a solicitação de inclusão de aplicações na base de assinaturas de aplicações;
81. Deve alertar o usuário quando uma aplicação for bloqueada;
82. Deve possibilitar a diferenciação de tráfegos Peer2Peer (Bittorrent, emule, etc) possuindo granularidade de controle/políticas para os mesmos;
83. Deve possibilitar a diferenciação de tráfegos de Instant Messaging (AIM, Hangouts, Facebook Chat, etc) possuindo granularidade de controle/políticas para os mesmos;
84. Deve possibilitar a diferenciação e controle de partes das aplicações como por exemplo permitir o Hangouts e bloquear a chamada de vídeo;
85. Deve possibilitar a diferenciação de aplicações Proxies (psiphon, freegate, etc) possuindo granularidade de controle/políticas para os mesmos;
86. Deve ser possível a criação de grupos dinâmicos de aplicações baseados em características das aplicações como: tecnologia utilizada nas aplicações (Client-Server, Browse Based, Network Protocol, etc);
87. 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;
88. Deve ser possível a criação de grupos estáticos de aplicações baseados em características das aplicações como: Categoria da aplicação.

Prevenção de ameaças:

89. Para proteção do ambiente contra ataques, os dispositivos de proteção devem possuir módulo de IPS, Antivírus e Anti-Spyware integrados no próprio appliance de firewall;
90. Deve incluir assinaturas de prevenção de intrusão (IPS) e bloqueio de arquivos maliciosos (Antivírus e Anti-Spyware);
91. Deve sincronizar as assinaturas de IPS, Antivírus, Anti-Spyware quando implementado em alta disponibilidade;
92. Deve implementar os seguintes tipos de ações para ameaças detectadas pelo IPS: permitir, permitir e gerar log, bloquear e manter em quarentena o IP do atacante por um intervalo de tempo;
93. As assinaturas devem poder ser ativadas ou desativadas, ou ainda habilitadas apenas em modo de monitoração;
94. Deve ser possível criar uma assinatura de IPS utilizando o identificador CVE assim como um "wildcard" do CVE para abranger mais de um identificador;
95. Deve ser possível a criação de políticas por usuários, grupos de usuários, IPs, redes ou zonas de segurança;
96. Exceções por IP de origem ou de destino devem ser possíveis nas regras ou assinatura a assinatura;
97. Deve suportar granularidade nas políticas de IPS, Antivírus e Anti-Spyware, possibilitando a criação de diferentes políticas por zona de segurança, endereço de origem, endereço de destino, serviço e a combinação de todos esses itens;
98. Deve permitir o bloqueio de vulnerabilidades;
99. Deve permitir o bloqueio de exploits conhecidos;
100. Deve incluir proteção contra ataques de negação de serviços;
101. Ser imune e capaz de impedir ataques básicos como: Syn flood, ICMP flood, UDP flood, etc;
102. Detectar e bloquear a origem de portscans;
103. Bloquear ataques efetuados por worms conhecidos;
104. Possuir assinaturas específicas para a mitigação de ataques DoS e DDoS;
105. Possuir assinaturas para bloqueio de ataques de buffer overflow;
106. Deverá possibilitar a criação de assinaturas customizadas pela interface gráfica do produto;
107. Deve permitir usar operadores de negação na criação de assinaturas customizadas de IPS ou anti-spyware, permitindo a criação de exceções com granularidade nas configurações;
108. Permitir o bloqueio de vírus e spywares em, pelo menos, os seguintes protocolos: HTTP, FTP, SMB, SMTP e POP3;
109. Identificar e bloquear comunicação com botnets;
110. Registrar na console de monitoração 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;
111. Deve possuir a função de proteção a resolução de endereços via DNS, identificando requisições de resolução de nome para domínios maliciosos de botnets conhecidas;
112. Os eventos devem identificar o país de onde partiu a ameaça;
113. Deve incluir proteção contra vírus em conteúdo HTML e javascript, software espião (spyware) e worms;
114. Possuir proteção contra downloads involuntários usando HTTP de arquivos executáveis e maliciosos;
115. Deve ser possível a configuração de diferentes políticas de controle de ameaças e ataques baseado em políticas do firewall considerando usuários, grupos de usuários, origem, destino, zonas de segurança, etc, ou seja, cada política de firewall poderá ter uma configuração diferente de IPS, sendo essas políticas por Usuários, Grupos de usuário, origem, destino, zonas de segurança;
116. Deve ser capaz de mitigar ameaças avançadas persistentes (APT), através de análises dinâmicas para identificação de malwares desconhecidos;
117. A solução de sandbox deve ser capaz de criar assinaturas e ainda inclui-las na base de antivírus do firewall, prevenindo a reincidência do ataque;
118. A solução de sandbox deve ser capaz de incluir no firewall as URLs identificadas como origens de tais ameaças desconhecidas (Block list), impedindo que esses endereços sejam acessados pelos usuários de rede novamente;
119. Dentre as análises efetuadas, a solução deve suportar antivírus, query na nuvem, emulação de código, sandboxing e verificação de call-back;
120. A solução deve analisar o comportamento de arquivos suspeitos em um ambiente controlado.

Filtro de URLs:

121. Permite especificar política por tempo, ou seja, a definição de regras para um determinado horário ou período (dia, mês, ano, dia da semana e hora);
122. Deve ser possível a criação de políticas por grupos de usuários, IPs, redes ou zonas de segurança;
123. Deve possuir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais URLs através da integração com serviços de diretório, Active Directory e base de dados local;
124. 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;
125. Suportar a capacidade de criação de políticas baseadas no controle por URL e categoria de URL;
126. Possuir pelo menos 60 categorias de URLs;
127. Deve possuir a função de exclusão de URLs do bloqueio;
128. Permitir a customização de página de bloqueio.

Identificação de usuários:

129. Deve incluir a capacidade de criação de políticas baseadas na visibilidade e controle de quem está utilizando quais aplicações através da integração com serviços de diretório, autenticação via LDAP, Active Directory, E-directory e base de dados local;
130. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;

131. Deve possuir integração e suporte a Microsoft Active Directory para o sistema operacional Windows Server 2012 R2;
132. Deve possuir integração com Microsoft Active Directory para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários, suportando single sign-on. Essa funcionalidade não deve possuir limites licenciados de usuários;
133. Deve possuir integração com Radius para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em usuários e grupos de usuários;
134. Deve possuir integração com LDAP para identificação de usuários e grupos permitindo granularidade de controle/políticas baseadas em Usuários e Grupos de usuários;
135. Deve permitir o controle, sem instalação de cliente de software, em equipamentos que solicitem saída a internet para que antes de iniciar a navegação, expanda-se um portal de autenticação residente no firewall (Captive Portal);
136. Deve possuir suporte a identificação de múltiplos usuários conectados em um mesmo endereço IP em ambientes Citrix e Microsoft Terminal Server, permitindo visibilidade e controle granular por usuário sobre o uso das aplicações que estão nestes serviços;
137. Deve implementar a criação de grupos customizados de usuários no firewall, baseado em atributos do LDAP/AD.

Filtro de dados:

138. Permitir identificar e opcionalmente prevenir a transferência de vários tipos de arquivos (MS Office, PDF, etc) identificados sobre aplicações (HTTP, FTP, SMTP, etc);
139. Suportar identificação de arquivos compactados ou a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
140. Suportar a identificação de arquivos criptografados e a aplicação de políticas sobre o conteúdo desses tipos de arquivos;
141. Permitir identificar e opcionalmente prevenir a transferência de informações sensíveis, incluindo, mas não limitado a número de cartão de crédito, possibilitando a criação de novos tipos de dados via expressão regular.

Geolocalização:

142. Suportar a criação de políticas por geolocalização, permitindo o tráfego de determinado País/Países sejam bloqueados;
143. Deve possibilitar a visualização dos países de origem e destino nos logs dos acessos.

VPN:

144. Suportar VPN Site-to-Site e Cliente-To-Site;
145. Suportar IPSec VPN;
146. A VPN IPSec deve suportar 3DES;
147. A VPN IPSec deve suportar Autenticação MD5 e SHA-1;
148. A VPN IPSec deve suportar Diffie-Hellman Group 1, Group 2, Group 5 e Group 14;
149. A VPN IPSec deve suportar Algoritmo Internet Key Exchange (IKEv1 e v2);
150. A VPN IPSec deve suportar AES 128, 192 e 256 (Advanced Encryption Standard);
151. A VPN IPSec deve suportar Autenticação via certificado IKE PKI;
152. Deve possuir interoperabilidade com os seguintes fabricantes: Cisco, Check Point, Juniper, Palo Alto Networks, Fortinet, SonicWall;
153. Deve permitir que todo o tráfego dos usuários remotos de VPN seja escoado para dentro do túnel de VPN, impedindo comunicação direta com dispositivos locais como proxies;
154. Atribuição de DNS nos clientes remotos de VPN;
155. Suportar autenticação via AD/LDAP, certificado e base de usuários local;
156. Suportar leitura e verificação de CRL (certificate revocation list);
157. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Antes do usuário autenticar na estação;
158. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Após autenticação do usuário na estação;
159. Deve suportar que a conexão com a VPN seja estabelecida das seguintes formas: Sob demanda do usuário;
160. Deverá manter uma conexão segura com o portal durante a sessão;
161. O agente de VPN IPSEC client-to-site deve ser compatível com pelo menos: Windows, MacOS e Linux.

SD-WAN:

162. A solução deve prover recursos de roteamento inteligente, definindo, mediante regras pré-estabelecidas, o melhor caminho a ser tomado para uma aplicação;
163. A solução deverá ser capaz de monitorar e identificar falhas mediante a associação de health check, permitindo testes de resposta por ping, http, tcp/udp echo e twamp;
164. Deverá ser permitida a criação de políticas de roteamento com base nos seguintes critérios: latência, jitter, perda de pacote, banda ocupada ou todos ao mesmo tempo;
165. Deve suportar o uso de VRF (Virtual Routing and Forwarding)
166. A solução deve permitir a definição do roteamento para cada aplicação;
167. Diversas formas de escolha do link devem estar presentes, incluindo: melhor link, menor custo e definição de níveis máximos de qualidade a serem aceitos para que tais links possam ser utilizados em um determinado roteamento de aplicação;
168. Deve possibilitar a definição do link de saída para uma aplicação específica;
169. Deve implementar balanceamento de link por hash do IP de origem;
170. Deve implementar balanceamento de link por hash do IP de origem e destino;
171. Deve implementar balanceamento de link por peso. Nesta opção deve ser possível definir o percentual de tráfego que será escoado por cada um dos links. Deve suportar o balanceamento de, no mínimo, dois links;
172. Deve implementar balanceamento de links sem a necessidade de criação de zonas ou uso de instâncias virtuais;
173. A solução de SD-WAN deve possuir suporte a Policy based routing ou policy based forwarding;
174. Para IPv4, deve suportar roteamento estático e dinâmico (BGP);
175. Deve possibilitar a agregação de túneis IPsec, realizando balanceamento por pacote entre os mesmos;
176. Deve possuir recurso para correção de erro (FEC), possibilitando a redução das perdas de pacotes nas transmissões;
177. Deve permitir a customização dos timers para detecção de queda de link, bem como tempo necessário para retornar com o link para o balanceamento após restabelecido;
178. Com a finalidade de controlar aplicações e tráfego cujo consumo possa ser excessivo, (como youtube, Facebook, etc), impactando no bom uso das aplicações de negócio, se requer que a solução, além de poder permitir ou negar esse tipo de aplicações, deve ter a capacidade de controlá-las por políticas de shaping. Dentre as tratativas possíveis, a solução deve contemplar:
179. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de origem;
180. Suportar a criação de políticas de QoS e Traffic Shaping por endereço de destino;
181. Suportar a criação de políticas de QoS e Traffic Shaping por usuário e grupo;
182. Suportar a criação de políticas de QoS e Traffic Shaping por aplicações;
183. Suportar a criação de políticas de QoS e Traffic Shaping por porta;
184. O QoS deve possibilitar a definição de tráfego com banda garantida. Ex: banda mínima disponível para aplicações de negócio;

185. O QoS deve possibilitar a definição de tráfego com banda máxima. Ex: banda máxima permitida para aplicações do tipo best-effort/não corporativas, tais como Youtube, Facebook etc;
186. Deve ainda possibilitar a marcação de DSCP, a fim de que essa informação possa ser utilizada ao longo do backbone para fins de reserva de banda;
187. O QoS deve possibilitar a definição de fila de prioridade;
188. Além de possibilitar a definição de banda máxima e garantida por aplicação, deve também suportar o match em categorias de URL, IPs de origem e destino, logins e portas;
189. A capacidade de agendar intervalos de tempo onde as políticas de shaping/QoS serão válidas é mandatória. Ex: regra de controle de banda mais permissivas durante o horário de almoço;
190. Uma vez que o tráfego é identificado, as políticas de shaping/QoS podem ser compartilhadas a todos os acessos que fizerem match na regra ou por IP. Ex: 10 Mbps de banda garantida por IP ou para todos os IPs que fizerem match na regra;
191. Deve possibilitar a definição de bandas distintas para download e upload;
192. A solução de SD-WAN deve prover estatísticas em tempo real a respeito da ocupação de banda (upload e download) e performance do health check (packet loss, jitter e latência);
193. A solução de SD-WAN deve suportar IPv6;
194. Deve possibilitar roteamento distinto a depender do grupo de usuário selecionado na regra de SD-WAN;
195. Deve ser capaz de bloquear acesso a aplicações;
196. Deve suportar NAT dinâmico bem como NAT de saída;
197. Deve suportar balanceamento de tráfego por sessão e pacote;
198. As funcionalidades de SD-WAN podem ser fornecidas no NGFW ofertado ou em uma solução à parte, na mesma quantidade de equipamentos definida para os firewalls;
199. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
200. Em caso de composição de solução, a solução de SD-WAN deverá suportar tráfego compatível com a capacidade do equipamento de firewall;
201. Deve implementar balanceamento de link por custo configurado do link;
202. Deve suportar o balanceamento de, no mínimo, 5 links;
203. Deve suportar o balanceamento de links de interfaces físicas, sub-interfaces lógicas de VLAN e túneis IPsec;
204. Deve suportar o balanceamento de links LTE (4G) sem restrições de uso, podendo ser usado em conjunto com outros links e não ser somente o backup para todos os outros links;
205. Deve gerar log de eventos que registrem alterações no estado dos links do SDWAN, monitorados pela checagem de saúde;
206. Deve suportar Zero-Touch Provisioning;
207. Possuir checagem do estado de saúde do Link baseando-se em critérios mínimos de: Latência, Jitter e Perda de Pacotes;
208. Deve ser possível configurar a porcentagem de perda de pacotes e o tempo de latência e jitter, na medição de estado de link. Estes valores serão utilizados pela solução para decidir qual link será utilizado;
209. A solução deve permitir modificar o intervalo de tempo de checagem, em segundos, para cada um dos links;
210. A checagem de estado de saúde deve suportar teste com Ping, HTTP e DNS;
211. Suportar UDP Hole Punching em arquitetura ADVPN;
212. A checagem de estado de saúde deve suportar a marcação de pacotes com DSCP, para avaliação mais precisa de links que possuem QoS configurado;
213. As regras de escolha do link SD-WAN devem suportar o reconhecimento de aplicações, grupos de usuários, endereço IP de destino e Protocolo;
214. Deve suportar a configuração de nível mínimo de qualidade (latência, jitter e perda de pacotes) para que determinado link seja escolhido pelo SD-WAN;
215. Deve suportar envio de BGP route-map para BGP neighbors, caso a qualidade mínima de um link não seja detectada pela checagem de saúde do link;
216. Deve ser possível utilizar o balanceamento round Robin na agregação de duas ou mais IPSEC VPNs determinando o peso para cada VPN;
217. Deve ser possível especificar o número mínimo de interfaces ativas em uma regra de SD-WAN para que esta regra seja válida.

ITEM 6 - SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO III

1. O serviço corresponde ao item 5.
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço de configuração será fornecido para a implantação do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 2.2. Este serviço deverá incluir avaliação de pré-implantação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implantação

- 3.1.1. 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.

3.2. Cronograma do plano de implementação

- 3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

- 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

- 3.4.1. 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;
- 3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

- 3.5.1. 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.
4. 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;
5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;
6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;

7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados;
8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
9. 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;
10. 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;
11. 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.

ITEM 7 - PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses

1. Ponto de acesso (AP) apropriado para uso interno, com garantia de 36 meses on-site, 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 UFPR;
2. Deve permitir configuração, gerenciamento e controle pela ferramenta de gerência Fortinet (Fortigate e Fortimanager), em produção na CONTRATANTE;
3. 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 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 e 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.

ITEM 8 - PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses

1. Ponto de acesso (AP) apropriado para uso interno, com garantia de 36 meses on-site, 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 UFPR;
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 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. Deve suportar os seguintes métodos de autenticação EAP: EAP-AKA, EAP-SIM, EAP-FAST, EAP-TLS, EAP-TTLS e PEAP;

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 ser gerenciado via SNMP;

46. Deve suportar consultas via REST API;

47. Deve possuir estrutura robusta para operação em ambientes internos e permitir ser instalado em paredes e tetos. Deve acompanhar os acessórios para fixação;

48. Deve ser capaz de operar em ambientes com temperaturas entre 0 e 45° C;

49. Deve suportar sistema antifurto do tipo Kensington Security Lock ou similar;

50. Deve possuir indicadores luminosos (LED) para indicação de status;

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 e 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.

ITEM 9 - PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses

1. Ponto de acesso (AP) apropriado para uso externo, com garantia de 36 meses on-site, 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 UFPR;

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 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 "não WiFi" 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 e 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.

ITEM 10 - INJETOR PoE (Power Injector)

1. Injetor PoE (power injector) para alimentação de dispositivos PoE onde não há switch com esta tecnologia, com garantia de 36 meses *on-site*;
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. Deve ser compatível com os itens 7, 8 e 9.

ITEM 11 - SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)

1. Solução de controle de acesso à rede, a ser ofertado em formato de appliance físico ou virtual, este que deverá estar disponível para as plataformas Vmware ESXi, AWS e Microsoft Azure;
2. Deve ser uma solução multi-vendor capaz de suportar os switches e concentrador VPN do órgão;
3. Deve suportar variadas soluções de Wi-Fi do mercado, tais como: Aruba, Ruckus, Cisco, Fortinet, Aerohive e Enterasys, pelo menos;
4. A solução deve ser capaz de inspecionar tanto IoT quanto estações/notebooks, sem depender de recursos como 802.1X e Mac-address bypass (MAB);
5. Para estações de trabalho, deve suportar verificação de compliance em VPN IPsec e SSL;
6. A licença contemplada deverá suportar todas as características exigidas neste termo de referência;
7. A solução deve permitir diferentes perfis de administração, com a capacidade de limitar e controlar a quantidade de acesso permitido às funcionalidades disponíveis, dependendo do grupo administrativo da organização ao qual o usuário pertence;
8. Deve detectar e classificar automaticamente o tipo dos dispositivos conectados na rede sem a necessidade de softwares instalados nos dispositivos;
9. Deve permitir determinar o perfil dos dispositivos descobertos por meio de métodos que não exigem a instalação de agentes, incluindo pelo menos os seguintes:

- i. Consultas em DHCP Fingerprint;
 - ii. Consultas via protocolos HTTP/HTTPS;
 - iii. Consultas via protocolo SNMP;
 - iv. Consultas via protocolo SSH;
 - v. Consultas via protocolo Telnet;
 - vi. Consultas de portas TCP;
 - vii. Consultas de portas UDP;
 - viii. MAC OUI;
 - ix. Consultas via protocolo WMI;
 - x. Protocolo ONVIF;
 - xi. Base assinaturas pré-definidas.
10. A solução deve ser capaz de reconhecer as seguintes informações sobre os dispositivos conectados à rede:
- i. Endereço MAC;
 - ii. Endereço IP;
 - iii. Sistema operacional;
 - iv. Nome do host;
 - v. Horário de conexão;
 - vi. Usuário conectado;
 - vii. Localização.
11. A solução deve ser capaz de reconhecer os seguintes sistemas operacionais em execução nos dispositivos conectados à rede:
- i. Android;
 - ii. Apple iOS para iPhone, iPod e iPad;
 - iii. Chrome OS;
 - iv. Linux;
 - v. MacOS X;
 - vi. Windows 7, 8 e 10;
12. Deve lembrar o perfil atribuído a cada dispositivo e verificar sua validade a cada conexão;
13. Deve permitir a designação de um sponsor para autorizar a categorização dos dispositivos;
14. Deve permitir a recategorização periódica de dispositivos;
15. Deve permitir a importação de um arquivo CSV contendo informações sobre os dispositivos a serem registrados;
16. A solução deve incluir a detecção de dispositivos desconhecidos conectados à rede e adotar medidas de controle para limitar o acesso;
17. A solução deve suportar autenticação através de EAP-PEAP e EAP-TLS;
18. A solução deve suportar RADIUS Change of Authorization;
19. A solução deve suportar MAC Address Bypass;
20. A solução deve consultar bases LDAP e Active Directory para a identificação de usuários e grupos de usuários;
21. A solução deve permitir a criação de políticas de controle que combinem informações sobre a identidade do usuário e tipo de dispositivo com objetivo de autorizar dinamicamente o acesso à rede;
22. Deve permitir a definição dos horários em que os dispositivos serão autorizados a conectar na rede;
23. Deve garantir a segmentação dinâmica da rede e aplicação de políticas de segurança, tendo como base variadas combinações, como login do AD e atributos (departamento, cidade, email, telefone), características da máquina (asset tag, hostname), localidade e horário;
24. A solução deve incluir recursos de gerenciamento de visitantes, permitindo a criação de diferentes perfis de utilização e autorização a serem associados aos usuários, distinguindo por exemplo prestadores de serviços dos visitantes;
25. A solução deve permitir o cadastro dos usuários visitantes na base interna da ferramenta para que não seja necessário realizar consultas em bases externas;
26. A solução deve possuir ferramenta que permita a geração automática de credenciais para usuários visitantes com login e respectivas senhas;
27. A solução deve possuir ferramenta que permita a criação de credenciais para eventos;
28. Deve permitir a definição de complexidade da senha dos usuários visitantes;
29. Deve ser possível definir um período de validade para as contas de usuários visitantes;
30. Deve ser possível definir data e horário para início e encerramento das contas de usuários visitantes;
31. A autenticação e autorização dos usuários visitantes deve ocorrer através de captive portal acessível via browser web;
32. Os visitantes em hipótese alguma deverão ter acesso à Internet e rede interna antes que a autenticação seja concluída e o usuário seja autorizado;
33. A solução deve vincular o login do visitante à máquina utilizada no acesso;
34. Deve suportar a validação de credenciais:
- i. Em base local interna à ferramenta;
 - ii. Em servidores RADIUS;
 - iii. Em servidores LDAP.
35. A solução deve autenticar usuários visitantes através das seguintes redes sociais: Facebook, LinkedIn e Twitter;
36. A ferramenta deve permitir que os usuários visitantes possam realizar auto-registro através do preenchimento de cadastro disponível em portal web;
37. Deve permitir a customização dos campos obrigatórios e opcionais para o cadastro de auto-registro;
38. A solução deve suportar o envio da senha de acesso aos visitantes através de SMS e e-mail;
39. Deve ser possível definir um período para que os usuários visitantes sejam obrigados a realizar nova autenticação;
40. Deve permitir a designação de grupos de usuários com função de sponsor que ficarão responsáveis por autorizar o acesso dos usuários visitantes e prestadores de serviços;
41. Os usuários do tipo sponsor poderão cadastrar previamente um usuário visitante. O portal de cadastro e gerenciamento de usuários visitantes não deve permitir gerência administrativa dos demais recursos da solução;
42. A solução deve permitir a customização da aparência do captive portal, permitindo editar textos e inserir imagens;
43. Os usuários do tipo sponsor podem ser cadastrados na base local da ferramenta ou fazer parte de grupo de usuários em base LDAP/Active Directory;
44. A solução deve incluir recursos de conformidade de endpoint. Antes de permitir que os dispositivos acessem a rede, a solução deve garantir que estes cumpram requisitos de segurança, integridade e conformidade;
45. Deve permitir o uso de software agente instalado no dispositivo e agentes evanescentes que não precisam ser instalados;
46. Tanto para IoTs quanto para estações de trabalho, se configurado, não devem ter qualquer acesso à rede de produção enquanto não forem inspecionados e identificados;
47. Se um dispositivo não passar os testes de conformidade, deve ser possível:
- i. Não forçar a remediação;
 - ii. Forçar a remediação imediatamente enviando o dispositivo à rede de quarentena;
 - iii. Permitir a remediação retardada, ou seja, dando um período de tolerância para que o usuário corrija o problema. Caso os problemas persistam, o dispositivo deve ser colocado em quarentena.

48. A solução deve permitir verificações de conformidade em endpoints que façam uso do sistema operacional:

- i. Windows 7;
- ii. Windows 8;
- iii. Windows 10;
- iv. MacOS;
- v. Linux.

49. Para garantir a conformidade com as políticas de segurança, a solução deve permitir que sejam verificados os seguintes itens antes de autorizar o acesso de um endpoint na rede:

- i. Presença de software de anti-vírus instalado e em execução;
- ii. Versão do sistema operacional;
- iii. Nome de domínio do Active Directory ao qual a estação Windows pertença;
- iv. Serviços em execução para estações Windows;
- v. Informações sobre um determinado certificado digital em estações Windows;
- vi. Registros ou chaves de registro para estações Windows;
- vii. Processos em execução para estações Windows, Linux e MacOS;
- viii. Arquivo armazenado em um determinado diretório para estações Windows, Linux e MacOS;
- ix. Pacotes instalados em estações Linux e MacOS.

50. A solução deve ser capaz de monitorar quando um serviço requerido for desabilitado ou interrompido em computadores. Além disso deve enviar a estação para quarentena de forma a garantir a conformidade com a política de segurança;

51. Deve possuir serviço RADIUS interno, além de permitir o uso de RADIUS externos;

52. Deve permitir a distribuição de agentes através de, pelo menos, os seguintes métodos:

- i. Programas de gerenciamento e distribuição de software;
- ii. GPO do Active Directory;
- iii. Captive Portal.

53. Deve permitir a atualização automática ou programada dos agentes instalados nas máquinas;

54. O agente instalado nos computadores deve notificar os usuários com mensagens informativas em casos de eventos;

55. Quando em quarentena, um portal web deve ser apresentado aos usuários com informações sobre as razões pelas quais estes foram movidos para o isolamento;

56. A solução deve compartilhar a identificação dos usuários e/ou dispositivos autenticados para a plataforma de segurança da rede via SSO, de forma que sejam vinculadas aos acessos de Internet, provendo rastreabilidade futura;

57. No que tange compliance, quando houver sucesso, falha ou alerta, a solução deve permitir as seguintes ações: alerta, envio de email e SMS, desabilitar o host, envio de mensagem direta para o host envolvido e executar políticas adicionais de compliance;

58. A solução deve integrar com plataformas de MDM, suportando pelo menos: FortiClient, In Tune, Mobile Iron e Air Watch;

59. Deve suportar integração com soluções de patching;

60. Deve suportar integração com soluções de análise de vulnerabilidades;

61. A solução deve possuir dashboard que apresente informações e estatísticas relevantes de forma resumida;

62. A solução deve permitir a customização do dashboard para apresentar as informações que o administrador considera relevante;

63. A solução deve permitir a consulta de informações e alteração de parâmetros de configuração via REST API;

64. A solução deve armazenar os eventos internamente e permitir que sejam exportados;

65. A solução deve permitir a exportação dos eventos através de syslog;

66. Deve suportar alta disponibilidade, suportando todos os registros e autenticações caso um nó da solução esteja indisponível;

67. A solução deve ser capaz de isolar hosts na quarentena mesmo quando estes estão conectados em redes de localidades remotas, tais como filiais. Não deve ser necessário estender a VLAN para isso;

68. Deve possuir registro dos eventos ocorridos na solução, bem como auditoria das configurações efetuadas;

69. Deve possibilitar o rastreamento de dispositivos, notificando a localização dos mesmos quando se conectarem à rede;

70. Dentre os relatórios disponibilizados pela solução dedicada de logs, deve suportar relatórios listando os endpoints por localidade e fabricante, usuários associados, além de relatórios de inventário, devices registrados e rogues;

71. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante;

72. 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.

ITEM 12 - LICENÇAS PARA SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO) PARA 1.000 DISPOSITIVOS

1. Licenciamento para a solução de controle de acesso à rede (item 11) operação com, pelo menos, 1.000 (mil) endpoints conectados simultaneamente;
2. A solução deve suportar capacidade de expansão conforme a necessidade da organização, sem demandar do cliente a troca do hardware/VM;
3. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante.

ITEM 13 - SERVIÇO DE CONFIGURAÇÃO PARA LICENÇA DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)

1. O serviço corresponde ao item 12.
2. Será configurado até 10% dos usuários conforme o licenciamento adquirido.
3. As instalações ocorrerão em etapas:
 - 3.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 3.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 3.3. Este serviço deverá incluir garantia de 3 (três) meses.

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 da contratada designado 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. Garantia de qualidade

4.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

4.4. Execução

4.4.1. 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;

4.4.2. A implementação será realizada remotamente.

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 de hardware 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;

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.

ITEM 14 - SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO

1. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS:

1.1. A solução deverá ser entregue em Appliance Virtual compatível com as plataformas VMware ESXi / ESX 4/5/6, Microsoft Hyper-V Server 2010, 2012 R2 e 2016, KVM e Xen. A responsabilidade pelo servidor/hardware com licenciamento necessário será da contratante;

1.2. Deverá ser entregue em solução virtual única ou com composição de soluções virtuais para atender as funcionalidades exigidas;

1.3. 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;

1.4. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante.

2. REQUISITOS GERAIS:

2.1. Suportar administração em interface gráfica (GUI) por HTTP e/ou HTTPS;

2.2. Suporta administração em interface baseada em linhas de comando (CLI) por TELNET e/ou SSH;

2.3. Permitir definir perfis de administradores para a solução, de modo que possa segmentar a responsabilidade dos administradores por tarefas operativas;

2.4. Possuir Indicador visual, centralizado, de informações críticas (estado da licença, versão de firmware, consumo de CPU/Memória/Disco, quantidade de usuários criados e licenciados);

2.5. Suportar a atualização do firmware via interface gráfica, por processo simplificado e intuitivo;

2.6. Suportar customização de mensagens padrão da solução como páginas de erro, portais de autenticação, auto registro, reset de senha e outros. Suportar também a inclusão, alteração e remoção de imagens nas mensagens/páginas sem a necessidade de recursos ou conectividade externa;

2.7. Suportar configuração de Alta Disponibilidade (HA), reduzindo ao máximo os períodos de interrupção;

2.8. Suportar implementações de HA como "Ativo-Passivo" ou sincronizando configurações entre duas caixas ativas;

2.9. Permitir sincronismo automático de configurações entre todos os equipamentos que componham a solução em HA;

2.10. Suportar implementação de HA sincronizando configurações com appliances em localidades geograficamente separadas;

2.11. Suportar a opção de backup criptografado;

2.12. Suportar backup automatizado (agendados por critérios pré-definidos), não somente sob demanda;

2.13. Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single-sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;

2.14. Suportar NTP (Network Time Protocol), visando o sincronismo de hora/data;

2.15. Suportar SNMP v1, v2 e v3 permitindo consultar MIB própria e envio de Traps;

2.16. Suportar nativamente Trap SNMP indicando mudança de status de HÁ;

2.17. Suportar captura de pacotes através da interface gráfica para Troubleshoot avançado em ferramentas de análise de pacotes (ex.: Wireshark);

2.18. O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, auto-registro de usuários e autenticação de segundo fator (token);

2.19. Deve suportar o envio de mensagens SMS para os usuários através de gateways SMS de terceiros ou seu próprio serviço de envio de SMS, sendo este segundo licenciado ou não;

2.20. Deve suportar o registro de todos os eventos que os usuários de sua base de dados local realizem com suas contas, tais como criação de um usuário, troca de senha de um usuário e alteração de informação gerais.

3. AUTENTICAÇÃO:

3.1. A solução deve efetuar autenticação para a gerência de identidade dos usuários da rede, ajudando a simplificar a administração dos mesmos sendo um ponto central de controle de autenticação, onde múltiplos métodos de autenticação possam ser consolidados;

3.2. Deve suportar autenticação em dois fatores (two-factor authentication);

3.3. Deve possuir suporte a autenticação de dois fatores em pelo menos dois tipos diferentes de tokens, sendo o primeiro físico (token), e o segundo lógico como software para dispositivos móveis, e-mail ou SMS, permitindo que seja dada a escolha de qual dos tipos utilizar para cada usuário;

3.4. A solução deve permitir que se defina um perfil de complexidade mínimo para as senhas de todos os usuários cadastrados na base de dados local, possibilitando a definição de número mínimo de letras minúsculas, letras maiúsculas, caracteres numéricos, caracteres especiais e etc;

- 3.5. A solução deve permitir a criação de política de bloqueio automático de usuários após uma quantidade de falhas de autenticação, assim evitando ataques de força bruta;
- 3.6. A solução deve suportar a criação de usuários em base local, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
- 3.7. A solução deve permitir a criação em massa de usuários na base de dados local através da importação de lista de usuários a serem criados contida em arquivos externos;
- 3.8. A solução deve permitir a criação de novos usuários na base de dados local e que o criador/administrador possa definir uma senha no momento de criação;
- 3.9. A solução deve permitir a criação de novos usuários na base de dados local de forma que o equipamento gere uma senha aleatória e envie automaticamente ao usuário;
- 3.10. A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;
- 3.11. Deve permitir associar os tokens aos usuários criados localmente na base de dados;
- 3.12. Deve permitir que os próprios usuários façam o registro dos seus tokens e relatem a perda de um token automaticamente, sem necessidade de envolver um administrador;
- 3.13. Remoção automática em massa de usuários desabilitados, baseado em critérios definidos;
- 3.14. A solução deve possuir formas que permitam que os usuários locais possam fazer o reset de suas senhas de forma segura sem a intervenção de administradores, através de correio eletrônico ou pergunta de segurança;
- 3.15. Deve suportar a criação de grupos de usuários, que poderão ser utilizados na autenticação dos dispositivos conforme necessidade;
- 3.16. Os tokens deverão gerar códigos com no mínimo 6 dígitos e intervalos não superiores a 60 segundos;
- 3.17. Suportar autenticação em dois fatores por hardware dedicado (Token);
- 3.18. Suportar autenticação em dois fatores por aplicativo mobile (iOS e Android);
- 3.19. Suportar autenticação em dois fatores por envio de mensagem SMS;
- 3.20. Suportar autenticação em dois fatores por envio de e-mail;
- 3.21. Suportar a sincronização com dispositivo em hardware de geração de OTP (One Time Password);
- 3.22. Deve permitir sincronizar os tokens com o equipamento para o correto funcionamento dos mesmos;
- 3.23. Deve permitir desabilitar um token quando este seja roubado ou extraviado, permitindo sua reativação posterior quando/se for recuperado;
- 3.24. Deve permitir a desassociação de um token a um usuário e associá-lo a outro usuário quando necessário, permitindo assim que sejam reaproveitados;
- 3.25. Deve continuar permitindo a autenticação de dois fatores em clientes Windows mesmo com a máquina offline;
- 3.26. Deve prover um portal web para o autorregistro dos usuários, de forma que o mesmo acesse, preencha os seus dados e submeta o registro. Após o usuário efetuar o registro, o administrador deverá ser notificado automaticamente para aprovar ou negar o cadastro do mesmo antes de que ele seja ativado;
- 3.27. A solução deve funcionar como servidor RADIUS (Remote Authentication Dial-In User Server), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
- 3.28. A solução deve suportar a integração com servidor RADIUS remoto;
- 3.29. A solução pode funcionar como servidor LDAP (Lightweight Directory Access Protocol), proporcionando autenticação aos dispositivos compatíveis com tal protocolo;
- 3.30. A solução deve suportar a integração com servidor LDAP remoto (como Microsoft Active Directory);
- 3.31. A solução deve suportar autenticação de usuários com credenciais de mídias sociais de terceiros como Facebook, Twitter, LinkedIn e Google+;
- 3.32. A solução deve permitir que usuários que não possuam uma conta local ou em mídias sociais se autenticuem através de um rápido cadastro, que garanta o mínimo de rastreabilidade, através da validação de endereços de e-mail ou número de telefone;
- 3.33. A solução deve permitir o login automático de usuários visitantes depois de se registrarem com sucesso;
- 3.34. A solução deve permitir configurar os parâmetros de rede (como as configurações de WiFi) em um endpoint baixando um script ou um executável através do portal de visitantes;
- 3.35. Deve suportar Security Assertion Markup Language (SAML), agindo como um Provedor de Identidade (Identity Provider - IDP) estabelecendo um relacionamento de confiança para autenticação segura de usuários tentando acessar um Provedor de Serviços (Service Provider - SP);
- 3.36. Deve permitir integração com bases do Azure Directory e GSuite;
- 3.37. Por meio do SAML, deve permitir integrações com SPs variados, tais como Office 365;
- 3.38. Deve suportar FIDO;
- 3.39. A solução deve apontar a última vez (data) em que um token foi utilizado;
- 3.40. A solução deve suportar OpenID Connect (OIDC);
- 3.41. Deve suportar autenticação adaptativa;
- 3.42. Deve suportar regras granulares no processo de autenticação. Ex: usuários se autenticando na VPN precisam utilizar MFA, mas, o mesmo usuário, em portal web, não precise informar o token;
- 3.43. Deve suportar push notification.

4. CONTROLE BASEADO EM PORTA:

- 4.1. A solução deve suportar nativamente (sem redirecionamentos) a integração e autenticação de switches e outros dispositivos compatíveis com o padrão 802.1X;
- 4.2. Suportar os seguintes métodos 802.1X EAP: PEAP (MSCHAPv2), EAP-TTLS, EAP-TLS e EAP-GTC;
- 4.3. Suportar interoperabilidade com equipamentos de acesso (switches) de outros fabricantes, para autenticação de portas junto a solução, através dos padrões 802.1X;
- 4.4. Deve suportar bypass de autenticação 802.1X para dispositivos conhecidos que não suportem 802.1X, a liberação deverá ser feita baseada no endereço MAC dos equipamentos previamente cadastrados, estes terão acesso à rede sem necessidade de autenticação ou ação do usuário ou dispositivo.

5. CERTIFICADOS:

- 5.1. A solução deve atuar como Autoridade Certificadora (CA);
- 5.2. Deve permitir a administração de certificados digitais, com emissão e revogação;
- 5.3. Deve permitir o uso de CA's confiáveis para validação de certificados emitidos por CA's externas;
- 5.4. Deve suportar OCSP para que se possa fornecer uma lista de certificados revogados (CRL);
- 5.5. Deve prover repositório para autenticação de VPN Site-to-Site através de Certificados;
- 5.6. Deve suportar SCEP Server (Simple Certificate Enrollment Protocol), permitindo a assinatura de requisições de certificados digitais (CSR) automaticamente ou com interação do administrador;
- 5.7. Deve ser capaz de importar outros certificados de CA's assim como a lista de certificados revogados;
- 5.8. Deve ser capaz de permitir ao administrador do sistema gerar, assinar e revogar certificados digitais para os usuários;
- 5.9. Suportar ao protocolo ACME para geração de certificados.

6. SERVIÇO DE AUTENTICAÇÃO ÚNICA (SINGLE SIGN-ON):

- 6.1. A solução deve prover capacidade de serviço SSO (Single Sign-On), com autenticação transparente (passiva) de usuários em sistemas compatíveis;

- 6.2. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio;
- 6.3. Deve permitir definir uma lista de usuários de SSO que serão ignorados, evitando assim interferência de contas de serviços tais como antivírus ou scripts via GPO;
- 6.4. Deve suportar análise de arquivos syslog enviados de fonte remota, para uso pelo serviço de SSO;
- 6.5. Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Identity Providers - IDP's) de terceiros;
- 6.6. Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On);
- 6.7. Deve suportar RSSO Accounting Proxy permitindo a recepção de pacotes radius de accounting, a modificação destes pacotes e o encaminhamento dos mesmos para vários outros pontos.

ITEM 15 - LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I (1.000 DISPOSITIVOS)

1. Deverá ser compatível e integrável com o item 14 deste termo;
2. Deverá possuir licenciamento para 1.000 (mil) usuários locais ou remotos;
3. Deverá possuir licenciamento para até 10 (dez) grupos de usuários;
4. Deverá possuir licenciamento para até 5 (cinco) certificados de usuários;
5. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante.

ITEM 16 - SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I

1. O serviço corresponde ao item 15;
2. Será configurado até 10% dos usuários conforme o licenciamento adquirido;
3. As instalações ocorrerão em etapas:
 - 3.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 3.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 3.3. Este serviço deverá incluir garantia de 3 (três) meses.

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 da contratada designado 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. Garantia de qualidade

- 4.3.1. A Contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

4.4. Execução

- 4.4.1. 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;
- 4.4.2. A implementação será realizada remotamente.

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 de hardware 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;
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.

ITEM 17 - LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II (10.000 DISPOSITIVOS)

1. Deverá ser compatível e integrável com o item 14 deste termo;
2. Deverá possuir licenciamento para 10.000 (dez mil) usuários locais ou remotos;
3. Deverá possuir licenciamento para até 10 (dez) grupos de usuários;
4. Deverá possuir licenciamento para até 5 (cinco) certificados de usuários;
5. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante.

ITEM 18 - SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II

1. O serviço corresponde ao item 17;
2. Será configurado até 10% dos usuários conforme o licenciamento adquirido;
3. As instalações ocorrerão em etapas:
 - 3.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 3.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 3.3. Este serviço deverá incluir garantia de 3 (três) meses.

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 da contratada designado 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. Garantia de qualidade

4.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

4.4. Execução

4.4.1. 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;

4.4.2. A implementação será realizada remotamente.

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 de hardware 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;

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.

ITEM 19 - SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX.

Características gerais da solução

1. Solução deve ser baseada em appliance físico ou virtual. Não serão considerados equipamentos de propósito genérico (PCs ou servidores) sobre os quais podem instalar-se e/ou executar um sistema operacional regular como Microsoft Windows, FreeBSD, SUN solaris ou GNU/Linux;
2. Ser capaz de atender a pelo menos 30.000 (trinta mil) caixas de e-mail (usuários);
3. Possuir capacidade mínima de atendimento diário a 1.0000.000 (um milhão) de e-mails e pico de 50 mil mensagens por hora sem enfileiramento, considerando o tamanho médio de mensagem como sendo de 100 (cem) KB;
4. A solução deve ser capaz de funcionar como gateway SMTP para os servidores de correio existentes;
5. A solução deve ser capaz de funcionar como gateway, atuando como MTA (Mail Transfer Agent);
6. A solução deve ser capaz de operar em modo transparente, atuando como um proxy transparente para o envio de mensagens aos servidores de correio protegidos;
7. Deve poder ser instalado como um proxy SMTP transparente, para a análise do correio de saída, procurando evitar o relatório na Blacklist;
8. A solução deve ter uma API baseada em REST disponível para fins de monitoramento, automação e orquestração;
9. A solução deve suportar listas brancas e listas negras (White/Black List) por usuários, por domínio e globalmente para todo o sistema;
10. A solução deve permitir a substituição, edição e personalização de mensagens de notificação de antivírus e anti-spyware;
11. A solução deve ser capaz de atrasar o envio de e-mail de grandes dimensões aos horários que são de menos carga;
12. A solução deve ser capaz de definir o encaminhamento de correio (relay) para um IP específico baseado no IP de origem da mensagem;
13. A solução deve fornecer suporte para múltiplos domínios de e-mail;
14. A solução deve suportar a implementação de políticas por destinatário, domínio, por tráfego de entrada ou de saída;
15. A solução deve ser capaz de entregar o correio baseado em usuários existentes em uma base LDAP;
16. A solução deve suportar quarentena por usuário, possibilitando que cada usuário possa administrar sua própria quarentena, removendo mensagens ou liberando as que não são SPAM, diminuindo a responsabilidade do administrador e também a possibilidade de bloqueio de e-mails legítimos. A quarentena deve ser acessada através de página Web e POP3;
17. A solução deve ser capaz de agendar o envio de relatórios de quarentena;
18. A solução deve ser capaz de realizar o armazenamento de e-mails (Archiving) baseado nas políticas de envio e recepção, com suporte também a armazenamento remoto;
19. A solução deve ser capaz de manter a fila de correio (Queue) em caso de falha na conexão de saída, atrasos ou erros de entrega;
20. A solução deve ser capaz de realizar a autenticação SMTP via LDAP, RADIUS, POP3 ou IMAP;

21. A solução deve ser capaz de manter listas de reputação do remetente com base em: quantidade de vírus enviados, quantidade de e-mails considerado spam, quantidade de destinatários equivocados;
22. A solução deve suportar direcionamento em IPv4 e IPv6;
23. Permitir a aplicação de políticas através dos filtros de conexões: Limite de número de mensagens por conexão, limite de número de destinatários por mensagem, limite do tamanho de mensagens e filtros de Reputação;
24. A solução deve permitir o armazenamento de e-mail e quarentena localmente ou servidor remoto;
25. A solução deve possuir funcionalidades de Antispam, Antivírus, Anti-Spyware e Anti-Phishing;
26. A solução deve ser capaz de realizar a inspeção de correio da Internet de entrada e saída;
27. A solução deve possuir um assistente (Wizard) para o provisionamento fácil e rápido de configurações básicas e domínios para proteger;
28. A solução deve oferecer proteção contra-ataques de negação de serviço como por exemplo Mail Bomb;
29. A solução deve fornecer controle de DNS reverso para proteção contra-ataques de Anti-Spoofing;
30. A solução deve se conectar em tempo real com a base de dados do fabricante para baixar atualizações Antispam;
31. A solução pode detectar se a origem de uma conexão é legal com base em um banco de dados de reputação de IP fornecido pelo fabricante;
32. A solução pode detectar se um e-mail é spam, verificando os URLs que contém, comparando-os com o banco de dados de reputação fornecido pelo fabricante;
33. A revisão de URLs deve permitir selecionar as categorias de URL que serão permitidas ou não, nos e-mails analisados. Este banco de dados de categorias será atualizado pelo fabricante;
34. A solução deve ter novos mecanismos de detecção de SPAM, através da análise contínua do correio recebido e sua correlação posterior com eventos ocorridos em todo o mundo, permitindo assim definir e detectar novas regras de SPAM;
35. A solução deve ser capaz de realizar a análise heurística e definir limites máximos de acordo com o compartilhamento de mensagens e assim determinar se um e-mail é spam;
36. A solução deve ser capaz de realizar análise Bayesiana para determinar se um e-mail é spam;
37. A solução deve ser capaz de detectar se o e-mail é um boletim de informação (Newsletter);
38. A solução deve ser capaz de filtrar e-mails baseados na URIs (Uniform Resource Identifier) contidos no corpo da mensagem;
39. A solução deve ser capaz de realizar análise com base em palavras proibidas (Banned Word);
40. A solução deve ter uma técnica que detecta SPAM através do uso de Greylist, que classifica o correio com base na sua entrada no início da sessão, como bloquear todos os e-mails e permitir apenas aqueles reenviados;
41. A solução permite criar uma Whitelist ou Blacklist de palavras;
42. A solução deve permitir o gerenciamento de spam com capacidade de aceitar, encaminhar (Relay), rejeitar (Reject) ou descartar (Discard);
43. A solução deve ser capaz de realizar análise de imagem e documentos PDF para a procura de spam;
44. A solução deve ser capaz de suportar listas negras (Blacklist) de terceiros;
45. A solução deve suportar greylist para contas de e-mail em IPv4 e IPv6;
46. A solução deve ser capaz de detectar endereços IP forjados (Forged IP);
47. A solução permite identificar imagens que fazem referência ao conteúdo SPAM. Ele deve suportar a análise das seguintes extensões GIF, JPEG, PNG;
48. A solução deve suportar Sender Policy Framework (SPF);
49. A solução deve suportar Domain Keys Identified Mail (DKIM);
50. A solução deve suportar Domain Based Message Authentication (DMARC);
51. A solução deve ser capaz de realizar uma inspeção profunda de cabeçalhos de e-mail;
52. A solução deve permitir sua configuração através de interface para acesso à Web (HTTP, HTTPS);
53. A solução deve ser capaz de permitir a criação de administradores exclusivos para a administração e configuração da solução por domínio, sendo também possível restringir o acesso por endereço IP e máscara de rede de origem;
54. A solução deve ser capaz de fornecer, pelo menos, dois níveis de acesso de gestão: Leitura/Gravação (Read/Write) ou somente leitura (Read Only);
55. A solução deve permitir a criação de perfis de configuração de forma granular, onde para cada perfil pode adicionar configurações específicas de funcionalidades como AntiSpam, antivírus, autenticação, entre outros;
56. A solução deve permitir esquemas de Alta Disponibilidade, tanto Active-Active quanto Active-Passive;
57. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de monitorar de status do link, suportar o Failover de rede e ser capaz de sincronizar as mensagens de quarentena de e-mails;
58. Quando a solução estiver implementada em alta disponibilidade Ativo/Passivo, deve ser possível sincronizar os dados de mensagens de e-mails e configurações;
59. Quando a solução estiver implementada em alta disponibilidade, deve ser capaz de detectar e notificar a falha de algum dispositivo;
60. A solução deve ter a capacidade de avaliar, reter e/ou bloquear e-mails que têm ameaças avançadas, Dia zero, através da análise com sandboxing;
61. Deve permitir análise de sandboxing com soluções na premissa ou na nuvem;
62. A solução deve ser capaz de filtrar anexos e conteúdo de e-mails;
63. A solução deve ser capaz de executar análise de antivírus/antispayware em arquivos compactados como ZIP, PKZIP, LHA, ARJ e RAR;
64. A solução deve ter uma base de informações de malware fornecida pelo fabricante e terceiros aliados, que podem ser atualizados de forma recorrente;
65. Após a detecção de um malware, a solução pode executar as seguintes ações: envie uma mensagem de notificação, reenviar mensagens e malwares para uma conta definida, reescreva o destinatário;
66. A solução deve ser capaz de verificar os e-mails que são liberados da quarentena SPAM pelo usuário em busca de conteúdo malicioso;
67. Deve suportar integração com o Microsoft 365 através de API;
68. Esta integração deve suportar a varredura pós-entrega sob demanda de e-mails no Microsoft 365 e também a varredura em tempo real, ou seja, as mensagens de e-mail devem ser verificadas logo após chegarem à caixa de correio do usuário;
69. Deve ser fornecido também uma solução de DLP, para detectar informações sensíveis que podem estar vindo através de e-mail;
70. A funcionalidade de DLP deve permitir especificar a informação a ser detectada como palavras, frases e expressões regulares, possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros, permitir a criação e armazenamento de impressões digitais (Fingerprint) de documentos e permitir a criação de filtros por arquivo;
71. A funcionalidade de DLP deve possuir uma lista predefinida de tipos de informações, como números de cartão de crédito e outros;
72. A funcionalidade de DLP deve permitir a criação e armazenamento de impressões digitais (Fingerprint) de documentos;
73. A solução deve suportar criptografia da mensagem baseada em identidade (Identity Based Encryption IBE) para que o destinatário não requeira uma PSK ou certificado instalado anteriormente para a descryptografado;
74. Criptografia de mensagens com IBE, deve suportar tanto o método push e pull, em que a mensagem criptografada é armazenada na plataforma de e-mail para acesso remoto autenticado ou ser enviado como anexo para o destinatário;
75. Em ambos os métodos da criptografia IBE, deve ter um registro do usuário do destino na plataforma de e-mail, de modo que, para ver as mensagens criptografadas, um processo de autenticação é necessário;
76. Deve suportar criptografia de e-mail usando S / MIME;
77. Suportar criptografado SMTPS e SMTP over TLS;
78. A solução deve analisar o conteúdo e anexos de uma mensagem em busca de palavras que indicam que a mensagem deve ser mantida em quarentena, criptografada, arquivada, bloqueada, marcada, substituída ou encaminhada para outro host;

79. Deve inspecionar arquivos protegidos por senha, usando senhas predefinidas, uma lista de senhas ou pesquisar a palavra password no corpo;
80. Deve ter a opção de remover ou neutralizar conteúdos potencialmente maliciosos e reconstruí-lo mais tarde. Por exemplo, em arquivos como o MSOffice e o PDF que possuem macros, java ou HTML com URLs mal-intencionados;
81. A solução deve ser capaz de armazenar logs e eventos localmente e também enviá-los para servidores remotos (Syslog);
82. A solução deve permitir o relato de atividade, analisando os arquivos de eventos (logs) e apresentá-los na tabela ou formato gráfico;
83. Permitir monitoramento via SNMP (Simple Network Management Protocol).
84. A solução deve permitir gerar relatórios sob demanda ou programados em intervalos de tempo específicos;
85. A solução deve permitir gerar e enviar relatórios em formato PDF ou HTML;
86. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante.
87. 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.

ITEM 20 - SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX.

1. O serviço corresponde ao item 19;
2. Serviço de configuração para pelo menos 30.000 (trinta mil) caixas de e-mail;
3. As instalações ocorrerão em etapas:
 - 3.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 3.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 3.3. Este serviço deverá incluir garantia de 3 (três) meses.

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 da contratada designado 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. Garantia de qualidade

4.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

4.4. Execução

4.4.1. 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;

4.4.2. A implementação será realizada remotamente.

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 de hardware 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;

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.

ITEM 21 - SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)

Características:

1. Suportar alta disponibilidade;
2. Suportar Disaster Recovery;
3. Executado como dispositivo ou VM hardening;
4. A solução PAM deve ser oferecida como baseada em dispositivo e deve ser fornecida pré-instalada com todos os softwares e serviços prontos para uso funcional;
5. A solução PAM não deve exigir conexão com a internet em qualquer capacidade;
6. Não deve ser possível para um usuário privilegiado sair do site com qualquer componente digital da solução;
7. Todos os componentes da solução PAM devem ser fornecidos em um estado protegido;
8. A solução PAM deve fornecer uma arquitetura de hardware totalmente redundante e capaz de funcionar no modo de failover HA e DR;
9. Todas as chaves de criptografia devem ser mantidas internamente na solução PAM reforçada;
10. A solução PAM deve empregar uma arquitetura de service broker;

11. A solução PAM deve expor uma API;
12. O processo de solicitação de senha deve ser aplicado apenas a senhas únicas;
13. Solicitações de senha devem ser possíveis usando infraestrutura mínima, não mais do que um dispositivo deve ser necessário para que a solução de proteção de senha seja totalmente funcional para solicitações de acesso de usuário privilegiado e gerenciamento de senha de sistemas de destino;
14. A solução PAM deve ser capaz de proteger as senhas de suas próprias contas de administração interna e disponibilizá-las usando um modelo de solicitação/liberação auditável;
15. Os critérios de gerenciamento de senha devem ser configuráveis para atender à política organizacional de frequência de alteração de senha/controle de aprovação de uso/alteração após o uso;
16. A solução PAM deve incluir e não se limitar aos seguintes recursos de Sistemas e Protocolos e Ferramentas:
 - AD;
 - Windows;
 - Linux/Unix;
 - Oracle DB;
 - MS SQL;
 - CISCO;
 - AS400;
 - Microsoft SQL;
 - Microsoft SQL Shell;
 - MySQL CLI;
 - MySQL Shell;
 - PostgreSQL CLI;
 - VNC;
 - WEB SMB;
 - WEB SSH;
 - Web RDP;
 - Web SFTP.
17. A solução PAM deve permitir a construção de um conector de plataforma personalizado e integração A2A;
18. O PAM deve oferecer suporte para aprovação de credencial dupla, exigindo aprovações de usuários designados antes de permitir o acesso a credenciais para contas gerenciadas;
19. O PAM deve suportar a capacidade de expirar a solicitação de aprovação após um período de tempo;
20. O PAM deve fornecer a capacidade de permitir recursos de checkout e check-in para secrets;
21. A solução PAM deve permitir a autenticação de uma sessão sem revelar a senha por meio da máquina do usuário final;
22. Sessões privilegiadas devem ser transmitidas por proxy por meio de um hardware seguro ou dispositivo virtual;
23. O proxy de sessão deve ser sem agente;
24. O proxy de sessão deve ser capaz de entrar em uma conta sem liberar uma senha para o usuário privilegiado;
25. As sessões devem permitir a inclusão ou exclusão de comandos executados durante uma sessão sem a necessidade de um agente;
26. A solução PAM deve suportar registro/monitoramento de pelo menos os seguintes protocolos de sessão - Telnet, SSH, RDP, ICA, VNC, SQL Plus, SQL Windows, Http & Https, x5250, x3270;
27. A solução PAM deve ser autoauditable, qualquer atividade do administrador da própria solução deve ser totalmente auditável;
28. As solicitações de acesso privilegiado devem ser feitas usando um modelo de solicitação/liberação, no mínimo;
29. Não deve ser possível para um administrador da solução realizar bypass do modelo de solicitação/liberação para obter uma senha ou ativar uma sessão;
30. A solução deve oferecer suporte à sessão remota de auditoria no modo não transparente ou transparente, sem alteração no fluxo de trabalho para acessar a sessão remota usando ferramentas nativas do cliente, incluindo injeção direta de credencial;
31. O PAM deve suportar monitoramento e gravação de sessão (para análise posterior) e monitoramento em tempo real (para vigilância em tempo real);
32. Deve ser possível gerar alertas de e-mail quando um usuário executa um comando restrito, a detecção de tais comandos deve ser sem agente;
33. As gravações de vídeo da sessão devem usar formatos disponíveis publicamente onde o codec é conhecido;
34. Não deve ser possível autenticar na API ou na interface de linha de comando da solução usando qualquer meio que não seja a criptografia baseada em chave;
35. A solução PAM deve ter suporte RADIUS para suporte MFA;
36. Os serviços não devem ser necessários para que a solução PAM seja implementada adequadamente, a solução proposta deve ser simples o suficiente para que a equipe existente integre a solução internamente;
37. A solução PAM deve suportar diferentes métodos de autenticação e integração com sistemas corporativos como: Active Directory, LDAP, SAML, Radius;
38. O PAM e o IAM devem ser fornecidos pelo mesmo fornecedor com integração pronta para uso;
39. O acesso do usuário final e o uso da solução devem ser possíveis usando APENAS uma interface web; isso inclui acesso a senhas, sessões e administração da solução;
40. A solução deve permitir controles ZTNA de usuários antes de acessar recursos, como verificações de identidade e verificações de postura do dispositivo;
41. A solução deve permitir a verificação de arquivos transportados do endpoint aos assets e vice-versa, protegidos pelo PAM via upload/download realizando scan de conteúdo malicioso;
42. A solução deve permitir a verificação de arquivos sendo baixados, use verificações DLP para garantir que informações confidenciais não possam ser movidas para o dispositivo do usuário;
43. Recurso que pode ser ativado para impedir a cópia da área de transferência de informações de recursos privilegiados;
44. Os patches devem ser devidamente testados e verificados pelo fornecedor antes de serem entregues em um formato criptografado e proprietário para garantir que apenas patches e alterações de código do fornecedor possam ser aplicados;
45. O PAM deve fornecer funcionalidade de break glass para emergências;
46. A solução deve ter tecnologia de firewall integrada;
47. A solução não deve permitir nenhum acesso ao software subjacente que suporta a solução de forma alguma;
48. O acesso do console aos dispositivos PAM deve ser restrito;
49. O acesso à rede para dispositivos PAM deve ser restrito;
50. Quaisquer serviços não utilizados ou desnecessários devem ser removidos de qualquer software de suporte para reduzir a superfície de ataque à segurança;
51. O licenciamento deve ser baseado em usuários que possuem privilégios de acesso aos ativos críticos protegidos pelo PAM;
52. A solução deve armazenar todas as senhas em um cofre seguro com criptografia AES-256;
53. A solução deve permitir que qualquer login/senha usados para acesso a servidores e máquinas remotos seja armazenado internamente e com segurança e permitir que os usuários se conectem aos sistemas de destino sem conhecimento de o login/senha utilizado;
54. A solução deve armazenar senhas e chaves SSH em um certified vault;
55. A solução deve alterar automaticamente as senhas para um grupo de recursos;
56. Gerenciamento avançado de senhas;

57. Ofereça um gerador de senha por política;
58. Estabeleça acesso granular a senhas;
59. Impedir que os usuários vejam a senha em texto simples;
60. A solução deve permitir que as credenciais sejam injetadas diretamente nos sistemas, dando acesso aos usuários sem que eles vejam ou forneçam credenciais;
61. Controle de acesso baseado em função;
62. Suporta controle de acesso sem VPN;
63. A solução deve permitir a gravação de sessões e salve as várias ações realizadas pelos usuários;
64. O vídeo gravado deve ser baixado no formato MP4;
65. Permita que um administrador monitore as sessões do usuário estabelecidas em tempo real e encerre as sessões, se necessário;
66. A solução deve permitir que as sessões sejam mantidas e compartilhadas com os auditores para interação (colaboração de sessão);
67. A solução deve permitir que os auditores monitorem usuários privilegiados sob demanda e em tempo real;
68. A solução deve integrar um sistema de fluxo de trabalho para permitir o acesso administrativo às máquinas identificadas;
69. A solução deve permitir acesso ao recurso de destino sem agente em (RDP, SSH, TELNET, VNC, HTTPS);
70. O usuário será bloqueado ao usar uma ação restrita;
71. Rastreabilidade de conexões;
72. Ver todas as conexões ativas;
73. Rastreabilidade e controle de transferências de arquivos;
74. A solução deve permitir uma notificação por e-mail em um determinado número de indicadores, como eventos relacionados ao tráfego (falha de conexão, falha de autenticação, etc.);
75. Autenticação com Active Directory;
76. A solução deve ser compatível com LDAPS;
77. A solução deve fornecer OTP via e-mail e gerenciamento de tokens para MFA integrado;
78. A solução deve ter integração com soluções SIEM para relatórios avançados e processamento em tempo real de detecção de comportamento malicioso;
79. A solução deve ter logs de auditoria completos e pesquisas avançadas, pesquisas de texto para isolar incidentes;
80. Os logs de auditoria da solução devem mostrar claramente quem acessou qual dispositivo de destino, bem como a duração (hora de início e hora de término);
81. A solução deve fornecer logs para o histórico de aprovação de sessões privilegiadas;
82. A solução deve ter um painel para exibir os usuários conectados no momento;
83. Ativar relatórios personalizáveis;
84. Gerenciamento de acesso privilegiado de 5 até 9 usuários;
85. Deve possuir garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante;
86. 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.

ITEM 22 - SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)

1. O serviço corresponde ao item 21;
2. Serviço de configuração para até 50 usuários;
3. As instalações ocorrerão em etapas:
 - 3.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 3.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 3.3. Este serviço deverá incluir garantia de 3 (três) meses.

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 da contratada designado 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. Garantia de qualidade

4.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

4.4. Execução

4.4.1. 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;

4.4.2. A implementação será realizada remotamente.

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 de hardware 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;

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.

ITEM 23 - PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO I (25GB/DIA)

1. Deve prover gestão centralizada dos logs dos equipamentos e ser necessariamente do mesmo fabricante do NGFW;
2. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi 7, Microsoft Hyper-V e Nutanix;
3. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante;
4. Deverá possuir a capacidade de receber pelo menos 25GB de logs diários;
5. O gerenciamento da solução deve suportar acesso via SSH, WEB(HTTPS) e API aberta;
6. Permitir acesso concorrente de administradores;
7. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP e RADIUS;
8. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
9. Deve registrar as ações efetuadas por quaisquer usuários;
10. O servidor de gerência deve ser hospedado em um equipamento/instância independente, não exercendo funções de firewall;
11. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
12. Deverá possuir mecanismos de apagamento automático para logs antigos;
13. Deverá permitir importação e exportação de relatórios;
14. Deverá ter a capacidade de criar relatórios no formato HTML;
15. Deverá ter a capacidade de criar relatórios em formato PDF;
16. Deverá permitir exportar os logs no formato CSV;
17. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
18. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;
19. Suportar o padrão SAML para autenticação do usuário administrador.

ITEM 24 - PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO II (500GB/DIA)

1. Deve prover gestão centralizada dos logs dos equipamentos e ser necessariamente do mesmo fabricante do NGFW;
2. Solução baseado em appliance ou em servidor virtualizado compatível com as seguintes plataformas de virtualização: VMware ESX/ESXi 7, Microsoft Hyper-V e Nutanix;
3. Deverá possuir garantia e licença para atualização de firmware e atualização automática de bases de dados de todas as funcionalidades pelo período de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante;
4. Deverá possuir a capacidade de receber pelo menos 500GB de logs diários;
5. O gerenciamento da solução deve suportar acesso via SSH, WEB(HTTPS) e API aberta;
6. Permitir acesso concorrente de administradores;
7. Deverá possuir autenticação de usuários para acesso à plataforma via LDAP e RADIUS;
8. Definição de perfis de acesso à console com permissões granulares como: acesso de escrita, acesso de leitura, criação de usuários, alteração de configurações;
9. Deve registrar as ações efetuadas por quaisquer usuários;
10. O servidor de gerência deve ser hospedado em um equipamento/instância independente, não exercendo funções de firewall;
11. Deve ser capaz de gerar relatórios ou exibir comparativos entre duas sessões diferentes, resumindo todas as alterações efetuadas;
12. Deverá possuir mecanismos de apagamento automático para logs antigos;
13. Deverá permitir importação e exportação de relatórios;
14. Deverá ter a capacidade de criar relatórios no formato HTML;
15. Deverá ter a capacidade de criar relatórios em formato PDF;
16. Deverá permitir exportar os logs no formato CSV;
17. Deverá permitir que os logs gerados pelos dispositivos gerenciados devem ser centralizados nos servidores da plataforma, mas a solução também deve oferecer a possibilidade de usar um servidor Syslog externo ou similar;
18. Deverá ser compatível com a autenticação de fator duplo (token) para usuários do administrador da plataforma;
19. Suportar o padrão SAML para autenticação do usuário administrador;
20. Deve possuir suporte para 36 (trinta e seis) meses.

ITEM 25 - SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS

1. O serviço corresponde aos itens 23 e 24;
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano.
 - 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implementação

3.1.1. 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.

3.2. Cronograma do plano de implementação

3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

3.4.1. 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.

3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

3.5.1. 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.

4. 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;

5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;

6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;

7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados;

8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;

9. 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;

10. 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;

11. 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.

ITEM 26 - PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL (ATÉ 10 FIREWALLS)

1. Solução que permita administrar de maneira centralizada todos os elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede dos campi e que garanta suporte a processos relativos à LGPD;

2. Deverá ser totalmente compatível com a solução proposta para gerenciamento da segurança e infraestrutura de rede dos campi;

3. A solução deverá estar devidamente licenciada para administrar todos os pontos de acesso, switches e elementos responsáveis pelo gerenciamento da segurança e infraestrutura de rede deste processo pelo período do contrato;

4. Quaisquer licenças e/ou softwares necessários para plena execução de todas as características descritas neste termo de referência deverão ser fornecidos;

5. A solução deverá ser composta por elemento ou elementos fornecidos na forma de appliance virtual (máquina virtual) compatível com Vmware ESXi, Microsoft Hyper-V ou Linux KVM;

6. A solução deverá garantir a integridade da configuração de um determinado item através de bloqueio de alterações quando ocorrer acesso simultâneo de dois ou mais administradores no mesmo ativo;

7. A solução deverá possibilitar a criação e administração de políticas de firewall, controle de aplicação e filtro de URL;

8. A solução deverá permitir criar, de forma centralizada, novos objetos que poderão ser utilizados nas políticas;

9. A solução deverá permitir que o administrador localize em quais regras um determinado objeto (ex: computador, serviço, etc.) está sendo utilizado;

10. A solução deverá atribuir sequencialmente um número a cada regra de firewall, de NAT ou de QoS;

11. A solução deverá permitir a criação de regras de filtragem de tráfego que fiquem ativas apenas em horários predefinidos;

12. A solução deverá permitir a criação de regras de filtragem de tráfego com data de expiração;

13. A solução deve possuir mecanismo de validação das políticas, avisando quando houver regras que ofusquem/conflitem com outras (shadowing) ou ainda garantir que esta exigência seja plenamente atendida por meio diverso;

14. A solução deve permitir a criação de templates de configuração de túneis VPN IPSec a serem aplicados de maneira centralizada e padronizada em elementos concentradores VPN;

15. A solução deve permitir agendamento para a execução de configurações nos elementos administrados;

16. A solução deve permitir a criação e execução de scripts em elementos administrados de maneira programada;

17. A solução deve permitir a criação de templates de configuração a serem aplicados de maneira centralizada e padronizada em elementos da rede sem fio e switches;

18. As seguintes características do SSID devem ser configuradas nos pontos de acesso através dos templates: nome do SSID, endereçamento DHCP a ser entregue aos clientes wireless, métodos de autenticação e agendamento da disponibilidade do SSID;

19. As seguintes características devem ser configuradas nos pontos de acesso através dos templates: potência de transmissão Wi-Fi, escolha do canal, tamanho do canal, configuração do algoritmo de seleção automática de potência e canal, configuração de short guard interval, modo de operação e acesso administrativo ao ponto de acesso;

20. As seguintes características de segurança devem ser configuradas na rede sem fio através dos templates: configuração da detecção de Rogue Aps e configuração de assinaturas de WIDS ou WIPS;

21. As seguintes características de Bluetooth Low Energy (BLE) devem ser configuradas nos pontos de acesso através dos templates: configuração do UUID, Major ID, Minor ID, Beacon Interval e potência;

22. As seguintes características de VLAN devem ser configuradas nos switches através dos templates: VLAN, VLAN ID e endereçamento IP;

23. As seguintes características de segurança devem ser configuradas nos switches através dos templates: Autenticação 802.1X, Autenticação MAB e Guest VLAN;

24. As seguintes características de rede devem ser configuradas nos switches através dos templates: configuração das portas com respectivas VLANs tagged e untagged, configuração do protocolo LLDP e configurações de QoS;

25. A solução deve permitir que o administrador selecione em quais elementos os templates de configuração deverão ser aplicados;

26. A solução deve listar os elementos administrados e seu status de operação;

27. A solução deve listar todos os clientes conectados na rede sem fio, o nome do ponto de acesso ao qual o cliente está conectado, qualidade do sinal da conexão de cada cliente, tipo de dispositivo utilizado na conexão e nome do SSID;

28. A solução deve listar todos os Rogue APs na rede sem fio, nome do SSID do propagado, canal impactado, nível de sinal detectado e nome do ponto de acesso que detectou o Rogue AP;

29. A solução deve incorporar mapa mundi para visão unificada do status de operação dos elementos. Deve ainda permitir a adição de planta baixa de múltiplas localidades;
30. A solução deve garantir visão centralizada do status e estatísticas de uso das interfaces dos switches;
31. A solução deve apresentar a topologia da rede com status dos elementos e informações sobre a atuação do protocolo Spanning Tree em interfaces;
32. A solução deve permitir a execução de testes remotos para identificação de problemas em cabos de rede conectados aos switches;
33. A solução deve permitir o agrupamento dos elementos administrados para aplicação de políticas ou templates de configuração;
34. A solução deverá realizar o backup automático das configurações dos elementos e permitir o retorno (rollback) de uma versão de configuração salva previamente;
35. A solução deverá possibilitar que o administrador visualize e compare diferentes versões de configurações dos elementos, sejam elas configurações vigentes, configurações anteriores e configurações antigas;
36. A solução deverá possuir sistema de backup e restauração de todas as configurações da própria ferramenta de administração centralizada;
37. A solução deverá identificar a versão de firmware em execução nos elementos administrados e garantir que quando houver novas versões de software para eles, que seja realizada a distribuição e instalação remota de maneira centralizada;
38. A solução deve permitir criar políticas/templates que definam a versão de firmware a ser distribuída e instalada em elementos administrados. Deve permitir ainda que o administrador da rede agende a atualização da versão de firmware de maneira automática nos elementos administrados;
39. A solução deverá implementar autenticação administrativa através dos protocolos RADIUS ou TACACS;
40. A solução deverá permitir a criação de múltiplos perfis de usuários administradores com permissões granulares para limitar o acesso a determinadas funções e garantir privilégios de somente leitura e/ou leitura-escrita a outras;
41. Garantia de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante. Durante o período de garantia deve ser possível a atualização do software para novas versões.
42. 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.

ITEM 27 - SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL

1. O serviço corresponde ao item 26;
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implementação

- 3.1.1. 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.

3.2. Cronograma do plano de implementação

- 3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

- 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

- 3.4.1. 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;
- 3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

- 3.5.1. 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.
4. 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;
5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;
6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;
7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da proponente e para os demais componentes que serão ofertados;
8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
9. 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;
10. 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;
11. 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.

ITEM 28 - SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES (LICENÇA DE 3 ANOS PARA 2.000 USUÁRIOS)

1. CARACTERÍSTICAS E FUNCIONALIDADES GERAIS:

- 1.1. A solução deverá ser entregue em Appliance Virtual compatível com as plataformas VMware ESXi / ESX 4/5/6, Microsoft Hyper-V Server 2010, 2012 R2 e 2016, KVM e Xen. A responsabilidade pelo servidor/hardware com licenciamento necessário será da contratante;

- 1.2. Deverá ser compatível e integrável com itens de autenticação centralizada do fabricante;
- 1.3. Deverá possuir licenciamento para 2.000 (dois mil) usuários locais ou remotos para o período de 36 (trinta e seis) meses com suporte técnico 24x7 do fabricante;
- 1.4. Deve possuir integração para acesso à Internet com autenticações 802.1X, em vários sistemas operacionais (iOS, Android, Microsoft Windows, Apple Mac OS X, ChromeOS) e dispositivos (laptops, smartphones, tablets).

2. REQUISITOS GERAIS:

- 2.1. Permitir definir perfis de administradores, segmentando a responsabilidade dos administradores por tarefas operativas;
- 2.2. Possuir um indicador visual de informações críticas (estado da licença, consumo de CPU/Memória/Disco, número de usuários e dispositivos conectados);
- 2.3. Suportar customização de mensagens padrão, como páginas de autenticação e reset de senha, com a inclusão de imagens sem necessidade de conectividade externa;
- 2.4. Suportar backup automatizado e criptografado, incluindo todas as configurações, base de usuários, grupos e políticas de autenticação;
- 2.5. Suportar o backup completo da configuração, incluindo base de usuários, grupos, tokens, certificados, configurações de single sign-on e etc. A solução deve também permitir a restauração de toda configuração diretamente da interface gráfica;
- 2.6. Suportar envio de e-mails e SMS para ações relacionadas a autenticação e notificações de segurança;
- 2.7. O equipamento deve permitir o envio de e-mails relacionados a reset de senha, aprovação de novos usuários, autorregistro de usuários e autenticação de segundo fator (token).

3. AUTENTICAÇÃO:

- 3.1. A solução deve efetuar autenticação para gerência de identidade de usuários da rede, consolidando múltiplos métodos de autenticação;
- 3.2. A solução deve permitir a criação de novos usuários na base de dados local sem a definição de senha, exigindo que o mesmo utilize o token como único fator de autenticação;
- 3.3. Deve suportar autenticação via redes sociais (Facebook, Google, LinkedIn), além de integração com Active Directory, RADIUS e Eduroam, OAuth 2.0 e OIDC, permitindo integração com bases de dados gov.br para autenticação na rede sem uso de ferramentas adicionais;
- 3.4. Suportar nativamente a integração e autenticação de dispositivos compatíveis com o padrão 802.1X;
- 3.5. Suportar métodos 802.1X como PEAP (MSCHAPv2), EAP-GTC e EAP-TLS, garantindo compatibilidade com diferentes fabricantes de switches e dispositivos de acesso;
- 3.6. Suportar o uso de protocolos como OCSP para assinatura e validação de certificados digitais;
- 3.7. A solução deve prover serviço SSO com autenticação transparente, integrando-se ao Active Directory para autenticação automática dos usuários já autenticados no domínio;
- 3.8. Deve ser capaz de integrar-se a um diretório ativo (Windows AD) e poder oferecer a funcionalidade de SSO, onde a autenticação automática/transparente via SSO para os serviços necessários é baseada na autenticação prévia feita pelo usuário no domínio;
- 3.9. Deve suportar Security Assertion Markup Language (SAML), agindo como autenticador de um Provedor de Serviços (Service Provider - SP) solicitando informações de identidade de usuários a Provedores de Identidade (Identity Providers - IDP's) de terceiros;
- 3.10. Deve suportar SSO baseado em Radius (RSSO - RADIUS Single Sign-On).

ITEM 29 – SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES

1. O serviço corresponde ao item 28;
2. As instalações ocorrerão em etapas:
 - 2.1. O serviço será fornecido para a configuração do dispositivo no ambiente da Contratada. Se o plano for fornecido pelo cliente ou proveniente de terceiros, a contratada apenas garantirá que o resultado da configuração esteja alinhado com o plano;
 - 2.2. Este serviço deverá incluir avaliação de pré-implementação, cronograma do plano de implementação, garantia de qualidade, execução e relatório;
 - 2.3. Este serviço deverá incluir garantia de 3 (três) meses.

3. Fases:

3.1. Avaliação de pré-implementação

- 3.1.1. 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.

3.2. Cronograma do plano de implementação

- 3.2.1. Após a avaliação, o especialista da contratada designado 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.

3.3. Garantia de qualidade

- 3.3.1. A contratante deverá garantir a qualidade por meio de testes em nosso laboratório com antecedência, para garantir que a solução possa ser implementada sem problemas. Uma variedade de testes será realizada para descobrir quaisquer problemas potenciais e mitigar quaisquer riscos com a implementação real.

3.4. Execução

- 3.4.1. 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;
- 3.4.2. A implementação será realizada remotamente.

3.5. Relatório de implementação

- 3.5.1. 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.
4. 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;
5. No caso de desativação de equipamentos legados, é de responsabilidade da Contratante a retirada dos equipamentos legados do ambiente no local de atendimento;
6. Será de responsabilidade do CONTRATANTE o fornecimento da conexão à Internet Mundial;
7. Será de responsabilidade do CONTRATANTE o fornecimento de energia elétrica para o equipamento LAN da PROPONENTE e para os demais componentes que serão ofertados;
8. Será de responsabilidade da CONTRATANTE disponibilizar a instalação física do equipamento de hardware em local adequado, assim como prover o acesso remoto a console de configuração do equipamento;
9. 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;
10. 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;

11. 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.

ITEM 30 – TRANSCEIVER 10GE SFP+ SR: Multimodo, LC Duplex, 300m

- 1. Transceiver SFP+ para conexão de fibras ópticas multimodo;
- 2. Deve ser compatível com o padrão 10GBASE-SR para fibras ópticas MM - Multimodo (300 metros);
- 3. Deve possuir conector LC Duplex;
- 4. Velocidade de 10Gbps;
- 5. Deve ser compatível com os itens 1, 3 e 5 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);
- 7. Deverá incluir garantia de 60 (sessenta) meses com suporte técnico 24x7 do fabricante.

ITEM 31 – TRANSCEIVER 10GE SFP+ LR: Monomodo, LC Duplex, 10km

- 1. Transceiver SFP+ para conexão de fibras ópticas monomodo;
- 2. Deve ser compatível com o padrão 10GBASE-LR para fibras ópticas SM – Monomodo (10 quilômetros);
- 3. Deve possuir conector LC Duplex;
- 4. Velocidade de 10Gbps;
- 5. Deve ser compatível com os itens 1, 3 e 5 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);
- 7. Deverá incluir garantia de 60 (sessenta) meses com suporte técnico 24x7 do fabricante.

ITEM 32 – TRANSCEIVER 40GE QSFP+ SR: Multimodo, MPO, 150m

- 1. Transceiver QSFP+ para conexão de fibras ópticas multimodo;
- 2. Deve ser compatível com o padrão 40GBASE-SR para fibras ópticas MM - Multimodo (150 metros);
- 3. Deve possuir conector Single 1x12 MPO;
- 4. Velocidade de 40Gbps;
- 5. Deve ser compatível com o item 1 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);
- 7. Deverá incluir garantia de 60 (sessenta) meses com suporte técnico 24x7 do fabricante.

ITEM 33 – TRANSCEIVER 40GE QSFP+ LR: Monomodo, LC Duplex, 10km

- 1. Transceiver QSFP+ para conexão de fibras ópticas monomodo;
- 2. Deve ser compatível com o padrão 40GBASE-LR para fibras ópticas SM - Monomodo (10 quilômetros);
- 3. Deve possuir conector LC Duplex;
- 4. Velocidade de 40Gbps;
- 5. Deve ser compatível com o item 1 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);
- 7. Deverá incluir garantia de 60 (sessenta) meses com suporte técnico 24x7 do fabricante.

ANEXO B - ENDEREÇOS DA UFPR NO PARANÁ

Região	Cidade	Identificação do Campus ou Unidade	Endereço	Distância aproximada a partir da Sede da Contratante	Tempo aproximado de viagem terrestre a partir da Sede da Contratante
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Centro Politécnico (SEDE)	Avenida Cel. Francisco H dos Santos, s/n, Jardim das Américas, Curitiba – PR, CEP:81530-900	-	-
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Complexo Reitoria	Rua XV de Novembro, 1299, Centro, Curitiba – PR, CEP: 80060-000	7,2km	13min

LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Setor de Ciências Agrárias	Rua dos Funcionários, 1540, Cabral, Curitiba – PR, CEP:80035-050	8,2km	18min
LOCALIDADE 1 Curitiba e região Metropolitana	Curitiba	Núcleo de Concursos	Rua dos Funcionários, 1540, Cabral, Curitiba – PR, CEP:80035-050	8,2km	18min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Departamento de Eng. Florestal	Avenida Pref. Lothário Meissner, 632, Jardim Botânico, Curitiba – PR, CEP: 80210-170	4km	9min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Setor de Ciências Sociais Aplicadas	Avenida Pref. Lothário Meissner, 632, Jardim Botânico, Curitiba – PR, CEP: 80210-170	4km	9min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Setor de Artes, Comunicação e Design Imprensa	Rua Bom Jesus, 650, Juvevê, Curitiba – PR, CEP: 80035-010	7,4km	16min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Prédio Histórico	Praça Santos Andrade, 50, Centro, Curitiba – PR, CEP: 80020-300	6,9km	19min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	PROGEPE	Rua Dr. Faivre, 590 - Centro, Curitiba – PR, CEP: 80060-000	6km	14min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	PRA	Rua Dr. Faivre, 105 - Centro, Curitiba – PR, CEP: 80060-000	6,5Km	15min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Setor de Educação Profissional e Tecnológica	Rua Dr. Alcides Vieira Arcoverde, 1225, Jardim das Américas, Curitiba – PR, CEP: 81520-260	1,1km	4min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Setor de Ciências da Saúde	Rua Padre Camargo, 280, Alto da Glória, Curitiba – PR, CEP: 80060-240	7,6km	18min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Sub sede Ciências da Saúde	Avenida Pref. Lothário Meissner, 632, Jardim Botânico, Curitiba – PR, CEP: 80210-170	4km	9min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Centro da Visão	Rua Pasteur, 26, Batel, Curitiba – PR, CEP: 80250-080	7,5km	18min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Departamento de Artes	Rua Cel. Dulcídio, 638 - Batel, Curitiba – PR, CEP: 80429-170	7,8km	19min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Campus Rebouças - Prédio Teixeira Soares	R. João Negrão, 940 – Centro, Curitiba – PR, CEP: 80230-150	5,9km	12min
Localidade 1 (Curitiba e Região Metropolitana)	Curitiba	Edifício Prof. Dr. José Munhoz De Mello	R. Ubaldino do Amaral, 321 - Alto da Glória, Curitiba – PR, CEP: 80060-195	7,3km	15min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Almoxarifado Central e Departamento de Educação Física	Rua Coração de Maria, 92 - Jardim Botânico, Curitiba – PR, CEP: 80210-132	5,1km	10min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Casa CREA	Rua Padre Camargo, 277, Centro, Curitiba – PR, CEP: 80060-240	7,6km	18min
LOCALIDADE 1 Curitiba e Região Metropolitana	Curitiba	Casa Amintas	Rua Amintas de Barros, 380 - Centro, Curitiba – PR, CEP: 80060-000	6,2km	16min

LOCALIDADE 1 Curitiba e Região Metropolitana	Pinhais	Fazenda Experimental do Canguiri	Rua Ivone Pimentel, 19, Jardim das Nascentes, Pinhais – PR, CEP: 83327-700	20,4km	25min
LOCALIDADE 1 Curitiba e Região Metropolitana	Piraquara	Campus Piraquara	Rod. Dep. João Lepoldo Jacomel, 4015, Jardim Primavera, Piraquara – PR, CEP: 83301-366	22km	19min
LOCALIDADE 2 Litoral do PR	Matinhos	Setor Litoral	Rua Jaguariaíva, 512, Caiobá, Matinhos - PR, CEP: 83260-000	107km	1h 28min
LOCALIDADE 2 Litoral do PR	Matinhos	Centro Cultural Setor Litoral e CENTRAN	Av. Paraná, 550, Tabuleiro, Matinhos - PR, CEP: 83260-000	106km	1h 24min
LOCALIDADE 2 Litoral do PR	Pontal do Paraná	Centro de Estudos do Mar	Avenida Beira Mar, s/n, Pontal do Sul – PR, CEP: 83255-976	114km	1h 53min
LOCALIDADE 2 Litoral do PR	Pontal do Paraná	Mirassol CEM Engenharia da Aquicultura	Rua Rio Grande do Norte, 145, Pontal do Paraná – PR, CEP: 83255-000	96,6km	1h 18min
LOCALIDADE 2 Litoral do PR	Paranaguá	Museu de Arqueologia e Etnologia da UFPR	Rua Quinze de Novembro, 575, Centro Histórico, Paranaguá – PR, CEP: 83203-010	85,5km	1h 15min
LOCALIDADE 3 Oeste do PR	Palotina	Setor Palotina	Rua Pioneiro, 2153, Dallas, Palotina – PR, CEP: 85950-000	599km	8h 22min
LOCALIDADE 3 Oeste do PR	Maripá	Extensão Setor de Palotina	Lote rural N°1.A1.B, 33º perímetro, Fazenda Britânia, Maripá – PR, CEP: 85955-000	580km	8h 5min
LOCALIDADE 3 Oeste do PR	Toledo	Campus Toledo	Rodovia PR 182, S/N, Km 320/321, Toledo – PR, CEP: 85919-899	555km	7h 35min
LOCALIDADE 3 Norte do PR	Jandaia do Sul	Campus Avançado de Jandaia do Sul	Rua Dr. João Maximiano, 426, Centro, Jandaia do Sul – PR, CEP: 86900-000	391km	6h 00min
LOCALIDADE 3 Sudeste do PR	Rio Negro	Estação Experimental de Rio Negro	BR 116, KM 206 - Tijucu Preto, Rio Negro – PR, 83880-000	110km	1h 42min

ANEXO C - TERMO DE COMPROMISSO E MANUTENÇÃO DE SIGILO

A **UNIVERSIDADE FEDERAL DO PARANÁ**, sediada à Rua XV de Novembro n.º 1299, nesta cidade de Curitiba, Estado do Paraná, CEP 80.060-000, CNPJ n.º 75.095.679/0001-49, doravante denominado CONTRATANTE, e, de outro lado, a <NOME DA EMPRESA>, sediada em<ENDEREÇO>, CNPJ n.º <CNPJ>, doravante denominada CONTRATADA;

CONSIDERANDO que, em razão da ATA DE REGISTRO DE PREÇOS N.º XX/20XX doravante denominado CONTRATO PRINCIPAL, a CONTRATADA poderá ter acesso a informações sigilosas da CONTRATANTE;

CONSIDERANDO a necessidade de ajustar as condições de revelação destas informações sigilosas, bem como definir as regras para o seu uso e proteção;

CONSIDERANDO o disposto na Política de Segurança da Informação da CONTRATANTE;

Resolvem celebrar o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO, doravante TERMO, vinculado ao CONTRATO PRINCIPAL, mediante as seguintes cláusulas e condições:

Cláusula Primeira – DO OBJETO

Constitui objeto deste TERMO o estabelecimento de condições específicas para regulamentar as obrigações a serem observadas pela CONTRATADA, no que diz respeito ao trato de informações sigilosas, disponibilizadas pela CONTRATANTE, por força dos procedimentos necessários para a execução do objeto do CONTRATO PRINCIPAL celebrado entre as partes e em acordo com o que dispõem a Lei 12.527, de 18/11/2011 e os Decretos 7.724, de 16/05/2012 e 7.845, de 14/11/2012, que regulamentam os procedimentos para acesso e tratamento de informação classificada em qualquer grau de sigilo.

Cláusula Segunda – DOS CONCEITOS E DEFINIÇÕES

Para os efeitos deste TERMO, são estabelecidos os seguintes conceitos e definições:

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

INFORMAÇÃO SIGILOSA: aquela submetida temporariamente à restrição de acesso público em razão de sua imprescindibilidade para a segurança da sociedade e do Estado.

CONTRATO PRINCIPAL: contrato celebrado entre as partes, ao qual este TERMO se vincula.

Cláusula Terceira – DA INFORMAÇÃO SIGILOSA

Serão consideradas como informação sigilosa, toda e qualquer informação classificada ou não nos graus de sigilo ultrassecreto, secreto e reservado. O TERMO abrangerá toda informação escrita, verbal, ou em linguagem computacional em qualquer nível, ou de qualquer outro modo apresentada, tangível ou intangível, podendo incluir, mas não se limitando a: know-how, técnicas, especificações, relatórios, compilações, código fonte de programas de computador na íntegra ou em partes, fórmulas, desenhos, cópias, modelos, amostras de ideias, aspectos financeiros e econômicos, definições, informações sobre as atividades da CONTRATANTE e/ou quaisquer informações técnicas/comerciais relacionadas/resultantes ou não ao CONTRATO PRINCIPAL, doravante denominados INFORMAÇÕES, a que diretamente ou pelos seus empregados, a CONTRATADA venha a ter acesso, conhecimento ou que venha a lhe ser confiada durante e em razão das atuações de execução do CONTRATO PRINCIPAL celebrado entre as partes;

Cláusula Quarta – DOS LIMITES DO SIGILO

As obrigações constantes deste TERMO não serão aplicadas às INFORMAÇÕES que:

I – sejam comprovadamente de domínio público no momento da revelação, exceto se tal fato decorrer de ato ou omissão da CONTRATADA;

II – tenham sido comprovadas e legitimamente recebidas de terceiros, estranhos ao presente TERMO;

III – sejam reveladas em razão de requisição judicial ou outra determinação válida do Governo, somente até a extensão de tais ordens, desde que as partes cumpram qualquer medida de proteção pertinente e tenham sido notificadas sobre a existência de tal ordem, previamente e por escrito, dando a esta, na medida do possível, tempo hábil para pleitear medidas de proteção que julgar cabíveis.

Cláusula Quinta – DOS DIREITOS E OBRIGAÇÕES

As partes se comprometem a não revelar, copiar, transmitir, reproduzir, utilizar, transportar ou dar conhecimento, em hipótese alguma, a terceiros, bem como a não permitir que qualquer empregado envolvido direta ou indiretamente na execução do CONTRATO PRINCIPAL, em qualquer nível hierárquico de sua estrutura organizacional e sob quaisquer alegações, faça uso dessas INFORMAÇÕES, que se restringem estritamente ao cumprimento do CONTRATO PRINCIPAL.

Parágrafo Primeiro – A CONTRATADA se compromete a não efetuar qualquer tipo de cópia da informação sigilosa sem o consentimento expresso e prévio da CONTRATANTE.

Parágrafo Segundo – A CONTRATADA compromete-se a dar ciência e obter o aceite formal da direção e empregados que atuarão direta ou indiretamente na execução do CONTRATO PRINCIPAL sobre a existência deste TERMO bem como da natureza sigilosa das informações.

I – A CONTRATADA deverá firmar acordos por escrito com seus empregados visando garantir o cumprimento de todas as disposições do presente TERMO e dará ciência à CONTRATANTE dos documentos comprobatórios.

Parágrafo Terceiro – A CONTRATADA obriga-se a tomar todas as medidas necessárias à proteção da informação sigilosa da CONTRATANTE, bem como evitar e prevenir a revelação a terceiros, exceto se devidamente autorizado por escrito pela CONTRATANTE.

Parágrafo Quarto – Cada parte permanecerá como fiel depositária das informações reveladas à outra parte em função deste TERMO.

I – Quando requeridas, as INFORMAÇÕES deverão retornar imediatamente ao proprietário, bem como todas e quaisquer cópias eventualmente existentes.

Parágrafo Quinto – A CONTRATADA obriga-se por si, sua controladora, suas controladas, coligadas, representantes, procuradores, sócios, acionistas e cotistas, por terceiros eventualmente consultados, seus empregados, contratados e subcontratados, assim como por quaisquer outras pessoas vinculadas à CONTRATADA, direta ou indiretamente, a manter sigilo, bem como a limitar a utilização das informações disponibilizadas em face da execução do CONTRATO PRINCIPAL.

Parágrafo Sexto - A CONTRATADA, na forma disposta no parágrafo primeiro, acima, também se obriga a:

I – Não discutir perante terceiros, usar, divulgar, revelar, ceder a qualquer título ou dispor das INFORMAÇÕES, no território brasileiro ou no exterior, para nenhuma pessoa, física ou jurídica, e para nenhuma outra finalidade que não seja exclusivamente relacionada ao objetivo aqui referido, cumprindo-lhe adotar cautelas e precauções adequadas no sentido de impedir o uso indevido por qualquer pessoa que, por qualquer razão, tenha acesso a elas;

II – Responsabilizar-se por impedir, por qualquer meio em direito admitido, arcando com todos os custos do impedimento, mesmo judiciais, inclusive as despesas processuais e outras despesas derivadas, a divulgação ou utilização das INFORMAÇÕES por seus agentes, representantes ou por terceiros;

III – Comunicar à CONTRATANTE, de imediato, de forma expressa e antes de qualquer divulgação, caso tenha que revelar qualquer uma das INFORMAÇÕES, por determinação judicial ou ordem de atendimento obrigatório determinado por órgão competente; e

IV – Identificar as pessoas que, em nome da CONTRATADA, terão acesso às informações sigilosas.

Cláusula Sexta – DA VIGÊNCIA

O presente TERMO tem natureza irrevogável e irretratável, permanecendo em vigor desde a data de sua assinatura até expirar o prazo de classificação da informação a que a CONTRATADA teve acesso em razão do CONTRATO PRINCIPAL.

Cláusula Sétima – DAS PENALIDADES

A quebra do sigilo e/ou da confidencialidade das INFORMAÇÕES, devidamente comprovada, possibilitará a imediata aplicação de penalidades previstas conforme disposições contratuais e legislações em vigor que tratam desse assunto, podendo até culminar na rescisão do CONTRATO PRINCIPAL firmado entre as PARTES. Neste caso, a CONTRATADA, estará sujeita, por ação ou omissão, ao pagamento ou recomposição de todas as perdas e danos sofridos pela CONTRATANTE, inclusive as de ordem moral, bem como as de responsabilidades civil e criminal, as quais serão apuradas em regular processo administrativo ou judicial, sem prejuízo das demais sanções legais cabíveis, conforme Art. 156 da Lei nº 14.133/21.

Cláusula Oitava – DISPOSIÇÕES GERAIS

Este TERMO de Confidencialidade é parte integrante e inseparável do CONTRATO PRINCIPAL.

Parágrafo Primeiro – Surgindo divergências quanto à interpretação do disposto neste instrumento, ou quanto à execução das obrigações dele decorrentes, ou constatando-se casos omissos, as partes buscarão solucionar as divergências de acordo com os princípios de boa-fé, da equidade, da razoabilidade, da economicidade e da moralidade.

Parágrafo Segundo – O disposto no presente TERMO prevalecerá sempre em caso de dúvida e, salvo expressa determinação em contrário, sobre eventuais disposições constantes de outros instrumentos conexos firmados entre as partes quanto ao sigilo de informações, tal como aqui definidas.

Parágrafo Terceiro – Ao assinar o presente instrumento, a CONTRATADA manifesta sua concordância no sentido de que:

- I – A CONTRATANTE terá o direito de, a qualquer tempo e sob qualquer motivo, auditar e monitorar as atividades da CONTRATADA;
- II – A CONTRATADA deverá disponibilizar, sempre que solicitadas formalmente pela CONTRATANTE, todas as informações requeridas pertinentes ao CONTRATO PRINCIPAL.
- III – A omissão ou tolerância das partes, em exigir o estrito cumprimento das condições estabelecidas neste instrumento, não constituirá novação ou renúncia, nem afetará os direitos, que poderão ser exercidos a qualquer tempo;
- IV – Todas as condições, TERMOS e obrigações ora constituídos serão regidos pela legislação e regulamentação brasileiras pertinentes;
- V – O presente TERMO somente poderá ser alterado mediante TERMO aditivo firmado pelas partes;
- VI – Alterações do número, natureza e quantidade das informações disponibilizadas para a CONTRATADA não descaracterizarão ou reduzirão o compromisso e as obrigações pactuadas neste TERMO, que permanecerá válido e com todos seus efeitos legais em qualquer uma das situações tipificadas neste instrumento;
- VII – O acréscimo, complementação, substituição ou esclarecimento de qualquer uma das informações disponibilizadas para a CONTRATADA, serão incorporados a este TERMO, passando a fazer dele parte integrante, para todos os fins e efeitos, recebendo também a mesma proteção descrita para as informações iniciais disponibilizadas, sendo necessário a formalização de TERMO aditivo ao CONTRATO PRINCIPAL;
- VIII – Este TERMO não deve ser interpretado como criação ou envolvimento das Partes, ou suas filiadas, nem em obrigação de divulgar INFORMAÇÕES para a outra Parte, nem como obrigação de celebrarem qualquer outro acordo entre si.

Cláusula Nona – DO FORO

A CONTRATANTE elege o foro do município de Curitiba, onde está localizada a sede da CONTRATANTE, para dirimir quaisquer dúvidas originadas do presente TERMO, com renúncia expressa a qualquer outro, por mais privilegiado que seja.

E, por assim estarem justas e estabelecidas as condições, o presente TERMO DE COMPROMISSO DE MANUTENÇÃO DE SIGILO é assinado pelas partes em 2 vias de igual teor e um só efeito.

Curitiba, _____ de _____ de 20____.

De Acordo

CONTRATANTE	CONTRATADA
<Nome> Matrícula: <Matr.>	<Nome> <Qualificação>
Testemunhas	
Testemunha 1	Testemunha 2
<Nome> <Qualificação>	<Nome> <Qualificação>

ANEXO D - TERMO DE CIÊNCIA

1 – IDENTIFICAÇÃO

ATA DE REGISTRO DE PREÇOS Nº	xxxx/aaaa		
OBJETO	Contratação de solução unificada de segurança e conectividade.		
CONTRATANTE	Universidade Federal do Paraná – UFPR	CNPJ	75.095.679/0001-49
GESTOR DO CONTRATO	<Nome do Gestor do Contrato>	MATR.	<xxxxxxxxxxxx>
CONTRATADA	<Razão Social da Contratada>	CNPJ	<xxxxxxxxxxxx>
PREPOSTO DA CONTRATADA	<Nome do Preposto da Contratada>	CPF	<xxxxxxxxxxxx>

2 – CIÊNCIA

Por este instrumento, os funcionários abaixo identificados declaram ter ciência e conhecer o inteiro teor do Termo de Compromisso de Manutenção de Sigilo e as normas de segurança vigentes da Contratante.

Funcionários da Contratada		
Nome	Matrícula	Assinatura
<Nome do(a) Funcionário(a)>	<xxxxxxxx>	
<Nome do(a) Funcionário(a)>	<xxxxxxxx>	
...	...	

Curitiba, <dia> de <mês> de <ano>.

ANEXO E - DECLARAÇÃO DE INEXISTÊNCIA DE REGISTRO DE OPORTUNIDADE

Pregão Eletrônico nº xx/20xx

A empresa _____, CNPJ _____, sediada em _____, declara que não realizou nenhum tipo de registro de oportunidade junto à Fortinet, tendo ciência de que esta prática é ilegal por ferir o princípio constitucional da isonomia e da seleção da proposta mais vantajosa para a Administração Pública, conforme disposto na Lei nº 14.133, de 2021.

Curitiba, ____ de _____ de 20xx

.....

Assinatura do representante legal

ANEXO F - DECLARAÇÃO DE GARANTIA

(Razão Social da Empresa), CNPJ nº XX.XXX.XXX/XXXX-XX, sediada xxxxxx, (endereço completo, telefone atualizados), por intermédio de seu representante legal, infra-assinado, declara, para fins de exigência do Edital de Pregão Eletrônico nº NNN/AAAA, que:

a) o prazo de garantia dos produtos será conforme a tabela abaixo, a contar do aceite definitivo dos bens ou serviços:

Item	Descrição	Marca	Quantidade	Métrica	Prazo de Garantia
1	<PREENCHER>	<PREENCHER>	2	Unidade	60 meses
3	<PREENCHER>	<PREENCHER>	2	Unidade	60 meses
5	<PREENCHER>	<PREENCHER>	2	Unidade	60 meses
7	<PREENCHER>	<PREENCHER>	1.100	Unidade	36 meses
8	<PREENCHER>	<PREENCHER>	100	Unidade	36 meses
9	<PREENCHER>	<PREENCHER>	20	Unidade	36 meses
10	<PREENCHER>	<PREENCHER>	50	Unidade	36 meses
30	<PREENCHER>	<PREENCHER>	24	Unidade	60 meses
31	<PREENCHER>	<PREENCHER>	12	Unidade	60 meses
32	<PREENCHER>	<PREENCHER>	16	Unidade	60 meses
33	<PREENCHER>	<PREENCHER>	6	Unidade	60 meses

- b) a garantia será prestada pelo Fabricante dos produtos e que o Fabricante está ciente e de acordo com o compromisso da prestação de garantia por nós assumido neste Edital;
- c) comprometemo-nos a prestar assistência técnica em função da garantia, incluindo manutenção corretiva, substituindo, conforme o caso, as peças ou equipamentos que apresentarem eventuais defeitos;
- d) estamos cientes de que a Administração da UFPR poderá recusar pedidos de extensão de prazo, de modo a cobrar pelo atraso, sem prejuízo de demais sanções cabíveis.

Informamos ainda, que, durante toda a vigência da garantia, a prestação dos serviços de manutenção descritos neste termo, ou no edital de licitação em questão, será realizada sem qualquer ônus à UFPR, sendo que essa deverá utilizar o(s) canal(ais) do Fabricante conforme abaixo:

Telefone:
Sistema de chamados:
E-mail:
Chat:

*Preencher somente dos dados pertinentes

Estamos cientes, também, de que nosso prazo para a troca/reposição de peças ou do próprio produto se inicia com a comunicação formal por parte da UFPR, a qual poderá se dar por telefone, e-mail ou através de sistema eletrônico de tratamento de chamados e, do mesmo modo, nos comprometemos a manter atualizados junto à UFPR os canais de comunicação que indicamos acima, sejam nossos ou de nossos credenciados/autorizados, bem como aqueles constantes de nossos cadastros.

_____, ____ de _____ de 20__.

Local e data

Assinatura do Responsável e carimbo da CONTRATADA

Dados da Empresa:	(CNPJ, razão social, endereço, telefone, correio eletrônico, nome do representante legal da empresa, nome do responsável pela assinatura da ata, número de telefone, fixo e/ou celular)
Dados para Pagamento:	(Banco, agência, número da conta corrente, praça de pagamento)

Item	Descrição	Marca /Fabricante /Modelo	Site do fabricante	Quantidade	Valor Unitário (R\$)	Valor Total (R\$)
01						
02						
03						
(...)						
VALOR TOTAL DA PROPOSTA (R\$)						

Do Detalhamento dos Custos de Fornecimento:

Item	Descrição	% Valor de aquisição	% Frete	% Impostos e Tributos	% Custos Indiretos e Lucro
01					
02					
03					
(...)					

Da forma de Entrega da Garantia do Contrato:

(X) Não se aplica (Não há exigência de garantia contratual)

- Validade da proposta: 90 (noventa) dias.
- Neste preço estão incluídas todas as despesas com impostos e outros.

Local e data.

Assinatura do Responsável

ANEXO II - ESTUDO TÉCNICO PRELIMINAR
PROCESSO ADMINISTRATIVO Nº 23075.049214/2024-91

CONTRATAÇÃO DE SOLUÇÃO UNIFICADA DE SEGURANÇA E CONECTIVIDADE

Histórico de Revisões			
Data	Versão	Descrição	Autor
31/10/2024	1.0	Finalização da primeira versão do documento	Equipe de Planejamento da Contratação

INTRODUÇÃO

O Estudo Técnico Preliminar – ETP é o documento constitutivo da primeira etapa do planejamento de uma contratação, que caracteriza o interesse público envolvido e a sua melhor solução. Ele serve de base ao Termo de Referência a ser elaborado, caso se conclua pela viabilidade da contratação.

O ETP tem por objetivo identificar e analisar os cenários para o atendimento de demanda registrada no Documento de Formalização da Demanda – DFD, bem como demonstrar a viabilidade técnica e econômica das soluções identificadas, fornecendo as informações necessárias para subsidiar a tomada de decisão e o prosseguimento do respectivo processo de contratação.

Referência: Inciso XI, do art. 2º e art. 11 da IN SGD/ME nº 94/2022.

1. INFORMAÇÕES BÁSICAS

Número do processo: 23075.049214/2024-91

2. DESCRIÇÃO DA NECESSIDADE DA CONTRATAÇÃO

2.1. Motivação/Justificativa

Diante dos desafios atuais enfrentados pela UFPR em relação à segurança da informação e conectividade, a implementação de soluções adequadas é essencial para garantir a continuidade, segurança e conformidade das atividades da universidade. A modernização da infraestrutura de rede é necessária para atender ao crescimento e às demandas atuais e futuras por conectividade segura. Além disso, o avanço na adoção das medidas recomendadas pelo Programa de Privacidade e Segurança da Informação (PPSI) permitirá à UFPR fortalecer a proteção de seus dados e sistemas críticos contra ameaças cibernéticas.

2.2. Contexto e Situação Atual

A Universidade Federal do Paraná (UFPR) é uma instituição de ensino e pesquisa de grande relevância, cuja infraestrutura de Tecnologia da Informação e Comunicação (TIC) desempenha papel essencial no suporte às suas atividades acadêmicas, administrativas e científicas. Em 2019, a UFPR implementou importantes medidas para proteger seus ativos digitais, incluindo uma solução de *firewall* instalada em 2019, composta por 2 equipamentos Fortinet 3200D e conjunto de funcionalidades, conforme Tabela 1.

Tabela 1 – Solução de *firewall* em uso

ITEM	PART NUMBER / ID DO PRODUTO	MODELO	TIPO DE PRODUTO
1	FG3K2D3Z16800150	FGT-3200D	HARDWARE
2	VDOM4713340541	FG-VDOM-15-UG	SOFTWARE
3	FG3K2D3Z16800341	FGT-3200D	HARDWARE
4	VDOM4713340540	FG-VDOM-15-UG	SOFTWARE

Contudo, a rápida evolução tecnológica e o crescimento das demandas institucionais impõem desafios significativos, especialmente no que tange à segurança da informação e à capacidade de expansão da rede. Adicionalmente, a falta de cobertura de suporte técnico, atualizações e garantia para os equipamentos de segurança de rede agrava o cenário, fragilizando a infraestrutura da universidade com a perda de funcionalidades essenciais. O recente diagnóstico da UFPR sobre os controles de segurança da informação, à luz das exigências estabelecidas no Programa de Privacidade e Segurança da Informação (PPSI) e Política de Segurança da Informação e Comunicação na UFPR (POSIC), revelou lacunas que precisam ser endereçadas para mitigar riscos de segurança cibernética. Entre os principais problemas estão a ausência de inventário e controle de ativos atualizados, além de deficiências em controles de acesso e autenticação. Outro aspecto crucial é a conectividade e segurança da rede sem fio da UFPR. Nos últimos anos, cada usuário passou a utilizar entre um e três dispositivos móveis, resultando em um aumento exponencial no número de dispositivos conectados. Esse crescimento intensificou a carga sobre os pontos de acesso existentes, sobrecarregando a capacidade da infraestrutura atual e ocasionando lentidão na navegação e indisponibilidade. Para garantir a continuidade e qualidade dos serviços é imprescindível atualizar e expandir a infraestrutura da rede sem fio da UFPR. Isso inclui a aquisição de novos equipamentos, modernização de software e hardware, e a implementação de estratégias que atendam às necessidades presentes e futuras da comunidade universitária (levantamentos realizados indicam a necessidade de aproximadamente 1.218 novos pontos de acesso). Diante desse quadro, a UFPR precisa de uma solução abrangente que atenda tanto as lacunas de segurança quanto as exigências de conectividade, alinhando-se às recomendações do PPSI e à necessidade de garantir a segurança e a integridade de seus dados e serviços. Os itens a serem licitados estão enquadrados como Solução de TIC, em atenção às disposições do Anexo I da Instrução Normativa SGD/ME nº 094/2022 - Licenciamento de software e serviços agregados; Aquisições de ativos de tecnologia da informação e comunicação. A partir das informações levantadas, pode-se classificar a contratação pretendida como comum, nos termos do Art. 6º da Lei 14.133/2021. Sendo que os itens não estão enquadrados como bens de luxo conforme trata o art. 20 de Lei nº 14.133/2021 e Decreto nº 10.818/2021.

2.3. Necessidade de Adequação às Diretrizes do PPSI e da POSIC

O Programa de Privacidade e Segurança da Informação (PPSI) e a Política de Segurança da Informação e Comunicação (POSIC) da UFPR estabelecem um conjunto de controles e orientações que visam assegurar a disponibilidade, integridade, confidencialidade e autenticidade das informações da universidade. Atualmente, a UFPR não implementa ou não está plenamente aderente a diversas dessas diretrizes, colocando em risco a segurança de dados, a proteção contra ameaças cibernéticas e a resiliência da infraestrutura de TIC. Este projeto de Solução de Segurança e Conectividade é justificado pela necessidade de:

- Atender às medidas de segurança do PPSI que ainda não foram implementadas.
- Proteger os dados sensíveis da instituição, garantindo conformidade com as regulamentações.
- Mitigar riscos de segurança, como vazamento de dados, invasões cibernéticas e acessos não autorizados.
- Modernizar a capacidade de conectividade e segurança da UFPR, alinhando-se às demandas de crescimento e de conectividade segura entre seus campi e datacenters.

2.4. Principais Medidas de Segurança do PPSI a Serem Atendidas

As medidas de segurança recomendadas pelo PPSI que ainda não foram implementadas de maneira completa na UFPR incluem:

2.4.1. Inventário e Controle de Ativos

PPSI Medida: Implementar um inventário automatizado de ativos de hardware e software, utilizando ferramentas de descoberta ativa e passiva.
POSIC Complemento: A POSIC destaca que a preservação dos ativos de informação é responsabilidade dos gestores e que o controle inadequado desses ativos pode levar à exposição indevida de informações.
Justificativa: A falta de controle sobre os ativos institucionais expõe a UFPR a riscos de uso de software desatualizado ou não autorizado, aumentando as vulnerabilidades da rede.

2.4.2. Proteção de Dados

PPSI Medida: Implementar criptografia de dados em trânsito e em repouso, tanto para dispositivos de usuário final quanto para mídias removíveis e sistemas críticos.

POSIC Complemento: A POSIC determina que a UFPR deve adotar tecnologias que garantam a **confidencialidade** das informações, protegendo dados sensíveis.

Justificativa: A UFPR ainda não implementou criptografia robusta, o que a deixa vulnerável a vazamentos e incidentes de segurança que poderiam comprometer informações pessoais e acadêmicas.

2.4.3. Controles de Acesso e Autenticação

PPSI Medida: Adotar controles de acesso rigorosos para acessos remotos e administrativos, além de centralizar a gestão de contas e sistemas de autenticação.

POSIC Complemento: A POSIC reforça a importância de controles de acesso eficazes, estabelecendo que apenas pessoas devidamente autorizadas devem ter acesso às informações da universidade, e que esses acessos precisam ser registrados e monitorados.

Justificativa: A falta de um controle centralizado de acessos expõe a instituição a vulnerabilidades que podem ser exploradas por ataques cibernéticos, comprometendo sistemas críticos da universidade.

2.4.4. Gestão de Vulnerabilidades e Patches

PPSI Medida: Implementar um processo contínuo de gestão de vulnerabilidades e de atualizações automáticas de software, incluindo a correção de vulnerabilidades identificadas por meio de varreduras regulares.

POSIC Complemento: A POSIC enfatiza a necessidade de proteger os sistemas contra vulnerabilidades conhecidas, por meio da aplicação regular de *patches* e da atualização de softwares e sistemas operacionais.

Justificativa: A falta de um processo estruturado de gestão de vulnerabilidades e *patches* deixa a UFPR suscetível a falhas de segurança, aumentando o risco de exploração por *malwares* e outras ameaças.

2.4.5. Registro e Monitoramento de Logs

PPSI Medida: Centralizar a coleta e o armazenamento de *logs* de auditoria, além de realizar análises contínuas para detectar atividades anômalas e incidentes de segurança.

POSIC Complemento: A POSIC estabelece que a UFPR deve garantir a **autenticidade** e **integridade** das informações por meio do monitoramento contínuo de acessos e atividades, assegurando que qualquer evento adverso seja devidamente registrado e analisado.

Justificativa: A ausência de um processo eficaz de monitoramento e análise de *logs* impede que a UFPR detecte e responda de forma proativa a ameaças cibernéticas e atividades anômalas.

2.4.6. Controle de malwares para E-mail

PPSI Medida: Implementar e manter proteção antimalware de servidor de e-mails.

POSIC Complemento: A POSIC estabelece que a UFPR deve garantir a **autenticidade** e **integridade** das informações por meio do monitoramento contínuo de acessos e atividades, assegurando que qualquer evento adverso seja devidamente registrado, analisado e tratado.

Justificativa: A ausência de solução automatizada de análise e tratamento em tempo real permite que contas sejam invadidas e utilizadas para propagação de malware, impondo riscos de segurança interna e prejudicando a reputação da instituição.

2.5. Objetivos do Projeto de Solução de Segurança e Conectividade

Este projeto visa implementar uma solução de segurança integrada que aborde as principais lacunas de segurança da UFPR, garantindo que a instituição esteja preparada para enfrentar as ameaças cibernéticas modernas, além de proteger adequadamente seus dados e ativos de informação. Os principais objetivos incluem:

Implementar controles de segurança robustos que assegurem a proteção de dados, incluindo criptografia, autenticação segura e segmentação de dados.

Contribuir para a automatização do inventário de ativos e softwares, permitindo um controle mais rigoroso sobre os sistemas e dispositivos conectados à rede da UFPR.

Realizar o monitoramento e análise do tráfego de rede para identificar e bloquear tentativas de intrusão e explorações de vulnerabilidades.

Fortalecer o monitoramento de *logs* e a gestão de vulnerabilidades, para garantir a detecção rápida de ameaças e a aplicação contínua de correções e atualizações de segurança.

Possibilitar a gestão centralizada de configurações e implementações de políticas de segurança na RedeUFPR.

Integrar a rede WLAN na solução de segurança, fortalecendo a proteção e a eficiência da RedeUFPR.

Aumentar a segurança da solução de e-mail corporativo, reduzindo a níveis mínimos a invasão de contas e as vulnerabilidades advindas.

Modernizar a infraestrutura de segurança para suportar o *backbone* de 40Gbps e a futura expansão para 100Gbps, garantindo uma solução escalável e com cobertura de suporte técnico.

Suporte técnico especializado para auxiliar na implantação, configuração, manutenção da solução e resolução de problemas.

2.6. Justificativa para a Solução Unificada

A implementação de uma solução integrada de segurança e conectividade permitirá à UFPR não apenas avançar em segurança, mas também modernizar sua infraestrutura de TIC de forma escalável e sustentável. Os benefícios de uma abordagem unificada incluem:

Eficiência Operacional: Ao integrar as medidas de segurança recomendadas pelo PPSI com a modernização da conectividade da universidade, a solução garantirá economia de escala, compatibilidade tecnológica e gestão centralizada, otimizando recursos orçamentários e humanos.

Racionalização de Custos: A adoção de uma solução única permite à UFPR realizar uma contratação consolidada, com suporte técnico especializado, reduzindo os custos operacionais a longo prazo e minimizando o risco de interrupções nas operações.

Resiliência e Conformidade: A solução proposta busca garantir a resiliência da infraestrutura da UFPR frente às crescentes ameaças cibernéticas, além de assegurar a conformidade com as exigências legais, como a LGPD e a Política Nacional de Segurança da Informação (PNSI).

Fortalecimento da Rede Sem Fio: A inclusão de *access points* na solução proporcionará a integração dos equipamentos e ferramentas de segurança para além da rede cabeada, bem como uma conectividade robusta e segura em todos os *campi* da UFPR, suportando a mobilidade dos usuários e a crescente demanda por acesso à internet de alta qualidade.

Capacidade de Expansão: A aquisição de equipamentos e soluções escaláveis permitirá à UFPR crescer conforme suas necessidades acadêmicas e administrativas, sem comprometer a segurança da informação ou a qualidade da conectividade.

2.7. Integração da rede WLAN a Solução de Segurança e Conectividade

A adição de *access points* no projeto de Solução de Segurança e Conectividade da UFPR é uma decisão estratégica que oferece vantagens, especialmente em um ambiente complexo e dinâmico como o da Universidade.

A contratação conjunta de soluções de segurança da informação e conectividade gera economia ao permitir melhores negociações com fornecedores, que oferecem pacotes integrados com descontos e licenciamento unificado. Equipamentos e infraestrutura também são compartilhados, simplificando o suporte e manutenção. O fornecimento de tais bens e serviços por diversos fabricantes acarretaria na impossibilidade de integração e, com isso, no aumento dos custos operacionais e infraestrutura física, bem como na complexidade de manter a solução em operação. Implicando também em aumento na demanda por capacidade técnica e recursos humanos, treinamento, curva de aprendizagem e custo total de propriedade.

Principais motivações para essa inclusão:

2.7.1. Integração Completa e Consistente da Segurança da Rede

Consistência nas Políticas de Segurança: Integrar *access points* com *firewalls* e outras ferramentas de segurança permite a aplicação consistente de políticas de segurança em toda a rede. Isso assegura que o tráfego seja submetido às mesmas regras de filtragem e inspeção, evitando brechas de segurança.

Gerenciamento Centralizado: A centralização da gestão facilita a configuração e a atualização de equipamentos, a integração e as implementações das políticas de segurança da RedeUFPR.

2.7.2. Aumento da Visibilidade e Controle sobre o Tráfego Sem Fio

Visibilidade Total do Tráfego : *Access points* modernos oferecem ferramentas avançadas de monitoramento que permitem visualizar e analisar o tráfego em tempo real. Isso facilita a detecção de comportamentos anômalos e possíveis tentativas de intrusão.

Análise de Comportamento: Com a integração com sistemas de detecção de intrusões (IDS) e prevenção de intrusões (IPS), os *access points* podem contribuir para uma análise mais aprofundada do comportamento da rede, identificando padrões suspeitos e mitigando ameaças proativamente.

2.7.3. Fortalecimento da Postura de Segurança através da Segmentação de Rede

Segmentação Avançada: *Access points* permitem a criação de múltiplas SSIDs (*Service Set Identifiers*) e VLANs (*Virtual Local Area Networks*), possibilitando a segmentação de diferentes tipos de tráfego (acadêmico, administrativo, convidados e IoT, como exemplos). Isso reduz a superfície de ataque e limita a propagação de possíveis ameaças.

Controle de Acesso Granular: Através da integração com soluções de Controle de Acesso à Rede (NAC), os *access points* podem aplicar políticas de acesso mais granulares, garantindo que apenas dispositivos e usuários autorizados acessem segmentos específicos da rede.

2.7.4. Melhoria na Resposta a Incidentes de Segurança

Deteção Precoce de Ameaças: Com monitoramento contínuo e análise em tempo real, os *access points* podem detectar e alertar sobre atividades suspeitas de forma imediata, permitindo uma resposta rápida para mitigar possíveis incidentes.

Facilidade em Auditorias: Ferramentas integradas de geração de relatórios e *logs* detalhados permitem uma documentação completa das atividades de rede, facilitando auditorias de segurança.

2.7.5. Facilitação da Implementação de Políticas de Segurança Dinâmicas

Suporte a Redes Convidadas Seguras: A criação de redes separadas para visitantes com acesso restrito garante que a segurança da rede principal não seja comprometida.

2.7.6. Potencial para Implementação de Tecnologias Emergentes

Preparação para o Futuro: Com a eminente adoção de dispositivos IoT na UFPR, os *access points* modernos são projetados para suportar uma vasta gama de dispositivos conectados, garantindo que a expansão tecnológica da universidade seja acompanhada por uma infraestrutura de segurança robusta.

2.7.7. Redução de Riscos e Eficiência Operacional

Prevenção de Incidentes de Segurança: Uma rede Wi-Fi bem protegida reduz significativamente o risco de incidentes de segurança que podem resultar em danos à reputação da instituição e interrupções operacionais.

Eficiência Operacional: A integração de *access points* com ferramentas de segurança permite uma gestão mais eficiente e proativa da infraestrutura de rede, reduzindo custos associados a respostas a incidentes e manutenção reativa.

2.8. WLAN

É premente a necessidade de modernizar e expandir a infraestrutura de rede sem fio (WLAN) da Universidade Federal do Paraná (UFPR), substituindo e complementando a rede cabeada existente, para atender de forma eficiente às crescentes demandas de conectividade de sua comunidade de mais de 46 mil usuários (alunos, servidores docentes, técnicos-administrativos e colaboradores terceirizados).

2.8.1. Objetivos Específicos para WLAN

Ampliação da Cobertura Wi-Fi em todos os campi da UFPR, eliminando pontos de sombra e garantindo conectividade em áreas críticas, incluindo salas de aula, laboratórios, bibliotecas, áreas administrativas e espaços externos.

Substituição e Complementação da Rede Cabeada: Reduzir a dependência da infraestrutura cabeada tradicional (que nos últimos anos tem demandado um investimento médio anual de R\$ 1.000.000,00), substituindo-a gradualmente por solução Wi-Fi que oferece maior flexibilidade e facilidade de expansão.

Aumento da Capacidade de Conexões Simultâneas: Incrementar a capacidade da rede para suportar um número maior de conexões simultâneas, superando as atuais 8.000 conexões, de modo a acomodar o crescimento contínuo de dispositivos na rede.

Melhoria do Desempenho da Rede: Assegurar velocidades de conexão adequadas para suportar aplicações exigentes como videoconferências, plataformas de ensino online, pesquisa acadêmica e administração institucional.

Fortalecimento da Segurança da Rede: Implementar as mais recentes medidas de segurança para impedir acessos não autorizados e garantir a integridade e confidencialidade das informações.

Escalabilidade e Flexibilidade da Infraestrutura: Projetar uma infraestrutura WLAN que possa ser facilmente expandida e adaptada às futuras necessidades tecnológicas da UFPR, incorporando soluções que suportem a evolução das demandas de conectividade e a integração de novas tecnologias.

Otimização da Gestão e Monitoramento da Rede: Facilitar a administração eficiente da rede Wi-Fi através de ferramentas de monitoramento e gestão, permitindo a identificação rápida de problemas, a otimização do desempenho e a manutenção proativa da infraestrutura.

Redundância e Confiabilidade: Incorporar mecanismos de redundância para garantir a continuidade do serviço de conectividade em caso de falhas de hardware ou outros imprevistos, assegurando a disponibilidade constante da rede para todas as atividades acadêmicas e administrativas.

3. ÁREA REQUISITANTE

Identificação da Área requisitante	Nome do responsável
Coordenadoria de Serviços e Infraestrutura de TIC (PRA/AGTIC/CSI)	Gustavo de Brito dos Santos

4. NECESSIDADES DE NEGÓCIO

Alinhamento ao [PDTIC 2022-2026](#):

ID	Objetivo Estratégico
OE.01	Posicionar a TIC como parceira estratégica da UFPR, contribuindo ativamente para o atingimento dos objetivos institucionais.
OE.02	Prover infraestrutura e demais recursos de TIC necessários, adequados às atividades finalísticas.
OE.03	Garantir melhoria contínua da qualidade da prestação de serviços de TIC.
OE.04	Garantir a segurança da informação e comunicação, a privacidade de informações sigilosas e demais aspectos da segurança institucional.

OE.05	Aprimorar a Gestão e fortalecer a Governança Digital.	
OE.07	Aprimorar o atendimento e conquistar altos índices de satisfação dos usuários e clientes de serviços digitais.	
OE.16	Promover a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).	
OE.17	Aumentar o iGovTI (Índice de Governança e Gestão de TI) e o iGestTI (Índice de Capacidade em Gestão de TI) a fim de contribuir para o aumento do IGG (índice Integrado de Governança e Gestão) estipulados pelo TCU.	
ID	Necessidade	Descrição da necessidade
NE.02	Manter a Infraestrutura de redes de dados.	Mapear, manter, suportar, prover atualização tecnológica e atender demandas por ampliação de toda a infraestrutura de rede de dados (metálica e ótica) da UFPR, incluindo ativos de rede, nobreaks e racks, etc., propiciando conectividade com disponibilidade.
NE.03	Manter, ampliar e melhorar a conectividade da rede sem fio corporativa (UFPR sem Fio).	Manter a rede sem fio da UFPR funcional, provendo suporte, renovação, ampliação, melhorias e ajustes nos serviços que garantam a disponibilidade e a conectividade para o acesso, facilidade de uso, segurança e a qualidade do serviço.
NE.12	Prover a segurança das informações e comunicações institucionais.	Prover os recursos e as soluções tecnológicas necessárias para implementar e manter a Política de Segurança da Informação (PSI) da UFPR.
NE.14	Reestruturar e manter ambientes de TIC em laboratórios e salas.	Prover suporte na estruturação e reestruturação de laboratórios de informática, assim como em salas de aula, relativamente a recursos de TIC.
NE.19	Implementar a Política de Segurança da Informação da UFPR pela TIC.	Implementar as determinações da PSI, provendo os recursos necessários, conforme Resolução nº 21/14-COPLAD, de 24/09/2014, que cria a Política de Segurança da Informação da UFPR (PSI/UFPR).
NP.03	Readequar e ampliar a rede sem fio corporativa (UFPR sem fio).	Readequar a rede sem fio da UFPR, promovendo constante atualização tecnológica, ampliação de cobertura conforme necessidade, inclusive para salas de aula, e provendo melhorias no atual serviço que garantam a disponibilidade e a conectividade para o acesso, facilidade de uso, segurança e a qualidade do serviço.
NP.11	Adequação dos assuntos relacionados à Tecnologia da Informação e Comunicação da UFPR à Lei Geral de Proteção de Dados Pessoais (LGPD).	Implementar as adequações de TIC, tais como aquelas relacionadas a sistemas de informação, bancos de dados, entre outros necessários ao atendimento dos requisitos impostos pela Lei nº 13.709, de 14 de agosto 2018.
NP.12	Prover soluções de cyber segurança para a UFPR.	Implementar soluções tecnológicas para proteger, monitorar e prevenir incidentes de segurança da informação, tais como ataques, invasões, acessos não autorizados, entre outros.

Alinhamento à Estratégia Federal de Governo Digital (EFGD) 2024-2027:

ID	Descrição
Objetivo 9	Elevar a maturidade e a resiliência dos órgãos e das entidades em termos de privacidade e segurança da informação.

Sobre o Plano de Contratações Anual

A presente contratação já está prevista no Plano de Contratação Anual de bens e serviços para 2024, devidamente homologada pela autoridade competente, conforme segue:

I) ID PCA no PNCP: 75095679000149-0-000001/2024

II) Data de publicação no PNCP: 19/05/2023

III) Id do item no PCA: Não informado (lançamento extemporâneo).

IV) Classe/Grupo:

·Classe 7050 - Equipamentos De Rede De Tic - Local E Remota.

·Grupo 166 - Serviços de Manutenção e Instalação de Equipamentos de TIC.

V) Identificador da Futura Contratação: 153079-443/2024

VI) Nome da Futura Contratação: Aquisição de solução unificada de segurança e conectividade.

Requisitos de negócio

As necessidades de negócio, também chamadas de requisitos do negócio, segundo o Corpo de Conhecimento de Análise de Negócios (*Business Analysis Body of Knowledge* - Guia BABOK® v3), são metas de mais alto nível, objetivos ou necessidades da organização. Descrevem as razões pelas quais um projeto foi iniciado, os objetivos que o projeto vai atingir e as métricas que serão utilizadas para medir o seu sucesso. Nesse sentido, a presente seção visa descrever as necessidades de negócios que conduzirão as análises de soluções e definição daquelas consideradas as mais adequadas a tais objetivos organizacionais, conforme relação a seguir:

- Atender às demandas institucionais, em especial a segurança da informação e ampliação da capacidade de cobertura de rede sem fio da UFPR de maneira totalmente integrada e com gestão unificada;
- Padronizar as especificações e disposições contratuais;
- Permitir a agregação de um volume significativo de demanda e, com isso, obter potencialmente melhores ofertas tanto em termos financeiros quanto técnicos;
- Assegurar que os equipamentos possuam garantia e suporte ao longo de sua vida útil, de maneira a evitar ou reduzir ao máximo a indisponibilidade de equipamentos e serviços;
- Prover apoio tecnológico à continuidade dos serviços desenvolvidos em cada unidade da UFPR (princípio da Continuidade do Serviço Público).

5. NECESSIDADES TECNOLÓGICAS

Segundo o Corpo de Conhecimento de Análise de Negócios (*Business Analysis Body of Knowledge* - Guia BABOK® v3), as necessidades tecnológicas, também chamadas de requisitos da solução de tecnologia, descrevem as características de uma solução que atende aos requisitos do negócio.

Dentre as necessidades tecnológicas dos equipamentos do presente estudo, destacam-se as seguintes:

- Resguardar os dados institucionais e sistemas críticos contra ameaças cibernéticas;
- Oferecer cobertura e desempenho da rede sem fio, agregando segurança, adequado às necessidades administrativas e finalísticas da UFPR;
- Atualizar a infraestrutura de TIC para sustentar o crescimento e as exigências futuras;
- Oferecer compatibilidade tecnológica e gestão unificada;
- Observar os requisitos ambientais.

6. DEMAIS REQUISITOS NECESSÁRIOS E SUFICIENTES À ESCOLHA DA SOLUÇÃO DE TIC

6.1. Requisitos de Garantia e Suporte/Assistência Técnica

Os equipamentos e softwares fornecidos deverão estar cobertos por garantia do fabricante no Brasil. A garantia deve incluir substituição de peças decorrente de vícios de projeto, fabricação, construção e montagem.

Todos os produtos fornecidos deverão ser novos e sem uso. Não serão aceitos materiais usados, remanufaturados ou de demonstração. Todos os componentes dos equipamentos deverão ser certificados pelo fabricante e devem estar em conformidade com a política de garantia.

O detalhamento dos procedimentos de suporte técnico e manutenção, assim como os níveis de serviço serão descritos no Termo de Referência.

6.2. Local de entrega

Os equipamentos deverão ser entregues conforme local especificado na Nota de Empenho. As entregas dos equipamentos de firewall e access points (APs) deverão ocorrer em Curitiba.

Os serviços de ativação dos equipamentos deverão ocorrer presencialmente, envolvendo atividades de planejamento, instalação, configuração e documentação.

A Agência de Tecnologia da Informação e Comunicação (AGTIC) está localizada no Centro Politécnico, à Rua Coronel Francisco Heráclito dos Santos, nº 100, Jardim das Américas – Curitiba/PR, CEP 81531-980, no 4º andar do Prédio de Administração.

6.3. Critérios e Práticas de Sustentabilidade

Foram consultados o Guia de Contratações Sustentáveis da AGU (6ª edição), os critérios de sustentabilidade ambiental contido no Art. 5º da Instrução Normativa nº 01, de 19 de janeiro de 2010, da Secretaria de Logística e Tecnologia da Informação do Ministério do Planejamento, Orçamento e Gestão - SLTI/MPOG e no Decreto nº 7.746/2012, da Casa Civil, da Presidência da República. No entanto não foram identificados outros critérios de sustentabilidade além daqueles eventualmente inseridos na descrição do objeto.

6.4. Das Condições de Habilitação

Para atendimento das condições de habilitação técnica, deverão ser apresentados os seguintes documentos:

a) **Termo de Compromisso e Manutenção de Sigilo;**

b) **Declaração de Garantia:** para os itens 1 a 10, a CONTRATADA deverá declarar aquisição da garantia junto ao fabricante para assegurar que os equipamentos estejam certificados e em conformidade com a política de garantia do fabricante. Deverá ainda indicar na proposta final o SKU ou *part number* dos equipamentos;

c) **Comprovante de que a empresa está relacionada como *partner*,** caso não seja ela própria o fabricante, atestando que a CONTRATADA é a representante autorizada, e está habilitada a comercializar, prestar serviços de instalação, configuração e suporte técnico aos equipamentos e softwares do fabricante, sem prejuízo da garantia. Essa exigência pode ser comprovada das seguintes formas:

i. indicação da página na Internet (URL do website) do fabricante que contenha esta informação; ou

ii. cópia do contrato entre a licitante e o fabricante; ou

iii. declaração do fabricante informando que a licitante é revendedora ou distribuidora autorizada.

d) **Atestado emitido por pessoa jurídica de direito público ou privado**, comprovando que a proponente fornece ou forneceu firewalls compatíveis com os itens 1, 3 ou 5. Também deverá ser apresentado documento comprovando que a proponente fornece ou forneceu pontos de acesso compatíveis com os itens 7, 8 e 9. Serão aceitos mais de um atestado para comprovação de capacidade técnica, devendo conter a identificação do emitente, em papel timbrado, com assinatura e informações para contato.

6.5. Da Qualificação Econômico-Financeira

Para a comprovação das condições de qualificação econômica financeira será exigida somente a certidão negativa de falência, ficando dispensadas as apresentações de balanço patrimonial e demais demonstrativos contábeis.

Para aferição da proposta dos itens 1, 3, 5, 7, 8, 9, 10, 11, 14, 17, 19, 21, 23, 24, 26, 28, 30, 31, 32 e 33 deverão ser apresentados os seguintes documentos:

a) **Catálogo e/ou ficha técnica do fabricante**, do qual se possa verificar as especificações técnicas e demais características do produto ofertado.

6.6. Do Seguro Garantia

Não será aplicado a previsão de garantia, nos termos do nos termos do Art. 96 da Lei 14.133/2021, dado não foram identificados riscos ou prejuízos à prestação dos serviços que necessitem de calços financeiros.

6.7. Da Participação de Consórcio ou Cooperativa

a) Será admitida a participação de empresas consorciadas na presente licitação.

b) Será permitida a participação de Cooperativas.

6.8. Da Subcontratação

Será vedada a subcontratação total ou parcial do objeto.

6.9. Da não reserva de cotas exclusivas à participação exclusiva de ME/EPP, de que trata o art. 48, inciso III da LC nº 123/2006

O art. 10 do Decreto 8.538/2015 estabelece que não se aplica o disposto nos art. 6º ao art. 8º quando, o tratamento diferenciado e simplificado para as microempresas e as empresas de pequeno porte não for vantajoso para a administração pública ou representar prejuízo ao conjunto ou ao complexo do objeto a ser contratado, justificadamente.

Considerando que a contratação é composta pelo agrupamento de materiais e serviços associados, não é possível estabelecer cotas que separem esse conjunto. Caso contrário, representariam prejuízo à perfeita execução do objeto. Cabe destacar que a reserva de cotas não pode ser aplicada aos itens de serviços e, além disso, os quantitativos demandados não permitem a aplicação do percentual de cota.

Sendo assim, os itens serão disputados pela ampla concorrência, visando maior competitividade e preços mais vantajosos para a Administração Pública, bem como a redução do risco de fracasso em alguns itens do processo licitatório.

6.10. Vedação da Participação de Pessoas Físicas

Considerando a necessidade de estrutura física indispensável para a entrega técnica e a prestação de serviços de manutenção corretiva e/ou preventiva, não será permitida a participação de pessoas físicas, com fulcro no Parágrafo único, do art. 4º, da Instrução Normativa SEGES/ME nº 116, de 21 de dezembro de 2021.

7. ESTIMATIVA DA DEMANDA – QUANTIDADE DE BENS E SERVIÇOS

Estima-se que a demanda atual é composta pelos itens elencados na Tabela 2, conforme necessidades apresentadas na seção “Descrição da necessidade da contratação”.

Tabela 2 – Estimativa da Demanda

Lote	Item	Descrição	Quantidade	Métrica	Fatores de Decisão / Justificativas
------	------	-----------	------------	---------	-------------------------------------

1	1	SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses.	2	Unidade	Renovar a proteção perimetral da RedeUFPR e incrementar a conectividade entre UFPR e RNP (equipamentos redundantes).
	2	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO I	2	Unidade	Configuração do Item 1.
	3	SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses.	2	Unidade	Segmentação da rede de datacenter (equipamentos redundantes).
	4	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO II	2	Unidade	Configuração do Item 3.
	5	SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses.	2	Unidade	Segmentação de ambientes não administrados pela AGTIC.
	6	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO III	2	Unidade	Configuração do Item 5.
	7	PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses.	1.100	Unidade	Necessidade de ampliação da rede Wi-Fi e integração da com as ferramentas de segurança. Quantitativos apurados com base na necessidade de substituição de equipamentos obsoletos e em <i>site surveys</i> realizados.
	8	PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses.	100	Unidade	Necessidade de ampliação da rede Wi-Fi e integração da com as ferramentas de segurança. Quantitativos apurados com base na necessidade de substituição de equipamentos obsoletos e em <i>site surveys</i> realizados.
	9	PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses.	20	Unidade	Necessidade de ampliação da rede Wi-Fi e integração da com as ferramentas de segurança. Quantitativos apurados com base na necessidade de substituição de equipamentos obsoletos e em <i>site surveys</i> realizados.
	10	INJETOR PoE (Power Injector)	50	Unidade	Quantidade estimada para utilização em localidades menores e que não dispõem de equipamentos com portas PoE.
	11	SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	1	Unidade	Implementar medidas para que os equipamentos utilizados por servidores em teletrabalho, não representem riscos à segurança ao acessar a rede e os sistemas institucionais.
	12	LICENÇAS PARA SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO) PARA 1.000 DISPOSITIVOS	5	Unidade	Implementação gradual da Solução de Controle de Acesso.
	13	SERVIÇO DE CONFIGURAÇÃO PARA LICENÇA DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	1	Unidade	Configuração do Item 11.
	14	SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO	1	Unidade	Aprimorar o gerenciamento de identidade e o controle de acesso.
	15	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I (1.000 DISPOSITIVOS)	5	Unidade	Implementação gradual da Solução de Gerenciamento de Identidade.
	16	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I	1	Unidade	Configuração do Item 15.
	17	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II (10.000 DISPOSITIVOS)	1	Unidade	Implementação gradual da Solução de Gerenciamento de Identidade.
	18	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II	1	Unidade	Configuração do Item 17.
	19	SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	1	Unidade	Sanar alto volume de credenciais comprometidas, bem como o grande esforço com remediação manual e tardia de ameaças entregues por e-mail. Quantidade estimada para proteger as contas Departamentais, de servidores TAEs e Docentes.
	20	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	1	Unidade	Configuração do Item 19.
	21	SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	2	Unidade	Necessidade de gerenciar, monitorar e proteger o acesso privilegiado a infraestrutura e sistemas críticos (contas de administradores que possuem permissões elevadas).
	22	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	1	Unidade	Configuração do Item 21.

23	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO I (25GB/DIA)	2	Unidade	Aprimorar a gestão e análise de logs de segurança de forma organizada, permitindo ações proativas para mitigar riscos e permitir resposta ágil à incidentes.
24	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO II (500GB/DIA)	1	Unidade	Incremento baseado no volume de logs atuais.
25	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS	1	Unidade	Configuração dos Itens 23 e 24.
26	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL (ATÉ 10 FIREWALLS)	1	Unidade	Implantar a gestão centralizada de configurações e implementações de políticas de segurança na RedeUFPR (FW + WLAN).
27	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL	1	Unidade	Configuração do Item 26.
28	SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES (LICENÇA DE 3 ANOS PARA 2.000 USUÁRIOS)	3	Unidade	Adequar o acesso para usuários externos à UFPR, incluindo participantes de eventos, feiras e visitantes, implementando o isolamento da rede de convidados para garantir a proteção dos recursos internos da universidade.
29	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES	3	Unidade	Configuração do Item 28.
30	TRANSCEIVER 10GE SFP+ SR: Multimodo, LC Duplex, 300m	24	Unidade	Interface para conexão de fibras ópticas. Quantitativo apurado para interconexão com o <i>backbone</i> da RedeUFPR.
31	TRANSCEIVER 10GE SFP+ LR: Monomodo, LC Duplex, 10km	12	Unidade	Interface para conexão de fibras ópticas. Quantitativo apurado para interconexão com o <i>backbone</i> da RedeUFPR.
32	TRANSCEIVER 40GE QSFP+ SR: Multimodo, MPO, 150m.	16	Unidade	Interface para conexão de fibras ópticas. Quantitativo apurado para interconexão com o <i>backbone</i> da RedeUFPR.
33	TRANSCEIVER 40GE QSFP+ LR: Monomodo, LC Duplex, 10km.	6	Unidade	Interface para conexão de fibras ópticas. Quantitativo apurado para interconexão com o <i>backbone</i> da RedeUFPR.

8. LEVANTAMENTO DE SOLUÇÕES

8.1. Soluções Identificadas

A Tabela 3 apresenta as soluções identificadas (cenários), com as respectivas vantagens e desvantagens.

Tabela 3 – Levantamento de Soluções

Descrição da Solução (ou Cenário)	Vantagens	Desvantagens
Solução 1: Contratação de serviço Consiste na contratação de serviços, em que serão fornecidos os equipamentos para uso por tempo determinado, ficando a responsabilidade de manutenção para a empresa contratada. Ao final do contrato a empresa contratada deverá recolher os equipamentos.	-Dispensa investimentos de capital (aquisição de bens) em estruturas internas para ter acesso à tecnologia de ponta. -Depreciação do equipamento é da empresa contratada. -Permite escalabilidade. -Todo o serviço envolvendo a solução, inclusive o gerenciamento, ficará sob responsabilidade da empresa contratada. -Não demanda tempo e recursos para capacitação de equipe própria. -Oferece profissionais especializados onde as melhores práticas do fabricante podem ser empregadas. -Desoneração de mão de obra operacional da UFPR. -Maior agilidade no tempo para atendimento e resolução de incidentes e problemas na rede.	-A contratante deverá prever orçamento para pagamento mensal/anual da solução sob o risco de ficar sem o serviço. -Alto risco de interrupção do funcionamento da rede no caso de atrasos nos pagamentos ou cancelamento do contrato. -A contratante ficará sujeita a atualização de preços do serviço fornecido, podendo tornar-se inviável a renovação do contrato. -Custo mais elevado por utilizar serviços e estruturas da contratada. -Complexidades para integrar os sistemas de gerenciamento dos recursos já existentes na instituição com os novos a serem contratados, havendo o risco da necessidade de gerenciar duas soluções distintas por dois responsáveis. -Necessidade de dar a terceiros o acesso ou até mesmo o controle sobre informações confidenciais do negócio. -Dependência da empresa para o funcionamento. -Transtornos e prejuízos com mudanças para restabelecer os serviços após o término ou rompimento do contrato.
Solução 2: Aquisição de equipamentos e softwares Consiste na aquisição e incorporação de bens materiais e softwares que compõem a solução, incluindo equipamentos de firewall, pontos de acesso (APs), licenciamento, serviços de configuração, garantia e suporte.	-Os bens pertencem à contratante e o uso se dará até o final da vida útil ou obsolescência tecnológica dos equipamentos. -Investimento gradativo, pois os componentes da solução podem ser adquiridos na medida que há disponibilidade de orçamento. -Maior controle sobre os riscos de interrupção dos serviços, já que todos os recursos são mantidos e gerenciados pela Universidade. -Menores riscos associados à exposição dos dados a terceiros em razão de menor necessidade de acesso ou controle sobre informações confidenciais do negócio pela Contratada.	-Após a garantia dos equipamentos, deverá ser contratado junto ao fabricante serviço de suporte e atualização. -A Universidade ficará sujeita a tecnologia contratada pelo período de viabilidade da solução. A troca por uma nova tecnologia implicará no desfazimento da solução adquirida anteriormente. -Onera mão de obra operacional da UFPR. -Implica maior tempo para atendimento e resolução de incidentes.

8.2. Soluções Disponíveis no Mercado

A Equipe de Planejamento da Contratação (EPC) identificou diversas soluções de mercado para atender a demanda por segurança da informação e conectividade. Nesse sentido, foram consultados relatórios especializados em tecnologia, como aqueles produzidos pelo Gartner.

Por meio de ferramentas como o quadrante mágico, profissionais de TI e gestores têm maior facilidade em tomar decisões, com objetivo de sustentar os negócios da instituição de modo mais eficiente.

O quadrante mágico Gartner é uma representação gráfica das atividades do mercado tecnológico em um determinado período de tempo. O relatório é muito útil para o desenvolvimento e aprimoramento da abordagem estratégica.

O quadrante mágico posiciona os players de mercado em 4 quadrantes: líderes, desafiadores, visionários e competidores de nicho. As empresas classificadas como "líderes" possuem uma credibilidade inigualável, pois demonstram uma sólida compreensão das necessidades do mercado e cumprem o compromisso de impulsionar o sucesso do cliente. Além disso, elas apresentam um modelo comercial atrativo, claro e sustentável.

A Equipe de Planejamento da Contratação avaliou os relatórios mais recentes divulgados pelo Gartner relacionados ao firewall de rede e infraestrutura de rede sem fio, respectivamente. Os relatórios trazem elementos que contribuem para uma tomada de decisão segura e assertiva em relação à escolha da solução a ser adotada.

O relatório "*Magic Quadrant for Network Firewalls*" é resultado da avaliação de 17 (dezessete) fornecedores de firewalls de rede. A Figura 1 apresenta o quadrante mágico com 3 (três) fornecedores posicionados como "líderes". São eles:

- Fortinet;
- Palo Alto Networks;
- Check Point Software Technologies.

Figura 1 – Magic Quadrant for Network Firewalls



Já o relatório "*Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure*" é resultado da avaliação de 12 (doze) fornecedores de infraestrutura de rede sem fio. A Figura 2 apresenta o quadrante mágico com 6 (seis) fornecedores posicionados como "líderes". São eles:

- Huawei;
- Cisco;
- Fortinet;
- Extreme Networks;
- HPE (Aruba);
- Juniper.

Figura 2 – Magic Quadrant for Enterprise Wired and Wireless LAN Infrastructure



Considerando a necessidade de aquisição de uma solução unificada, que envolve padronização de hardware/software, gestão centralizada e compatibilidade de tecnologias, verifica-se que o único fornecedor posicionado como “líder” em ambos os relatórios é a Fortinet.

Além disso, é importante mencionar o conhecimento prévio já existente na instituição a respeito da solução de firewall da Fortinet. A equipe já possui domínio das configurações, painéis de gestão e funcionalidades disponíveis na solução.

A Fortinet possui um portfólio completo para segurança da informação e conectividade. O firewall FortiGate possui integração com os pontos de acesso FortiAPs, além de integrações com solução de controle de acesso à rede (perímetro), gerenciamento de identidade e acesso, proteção de e-mail, gerenciamento de acesso privilegiado local (PAM), gerência centralizada de logs, identificação e autenticação de acesso de visitantes, entre outros.

A escolha do fabricante não caracteriza restrição a competitividade, visto que além de atender as características técnicas, dispõe de uma ampla rede de canais de distribuição, revenda e prestação de serviços autorizados no Brasil.

Em consulta realizada em 21/10/2024 no site do fabricante, disponível no endereço <<https://partnerportal.fortinet.com/directory/search?l=Brazil>>, foram listadas 100 (cem) empresas reconhecidas como Fortinet Partner.

Sendo assim, a Equipe de Planejamento da Contratação entende que esta é a solução mais adequada e trabalhará as especificações técnicas da solução Fortinet no Termo de Referência.

8.3. Formato da Contratação

A escolha da modalidade Pregão Eletrônico pelo Sistema de Registro de Preços encontra amparo nos incisos I, II e V do art. 3º do Decreto 11.462/2023, e se justifica pelas características do objeto, que necessita contratações frequentes; pela conveniência da contratação de serviços com previsão de entregas parceladas e pela natureza do objeto, em que não é possível definir previamente o quantitativo a ser demandado pela Administração. Esta modalidade também facilita o trabalho de planejamento orçamentário pela UFPR, possibilitando uma melhor aplicabilidade dos recursos ao longo do exercício.

9. ANÁLISE COMPARATIVA DAS SOLUÇÕES

A Tabela 4 apresenta a análise comparativa das soluções identificadas (cenários), em relação aos requisitos de negócio e tecnológicos.

Tabela 4 – Análise Comparativa das Soluções

Requisitos		Cenários	
		Solução 1	Solução 2
Negócio	Atender uma variedade de atividades institucionais que necessitam de infraestrutura de segurança da informação e conectividade.	Atende	Atende
	Atender todas as regiões no Estado do Paraná em que a UFPR possuir atividade.	Atende	Atende
	Permite ampliar a atual capacidade de processamento de dados.	Atende	Atende
	Baixo impacto na continuidade dos serviços caso ocorram cortes orçamentários.	Não atende	Atende
	Oferecer baixo risco de descontinuidade das atividades institucionais por falhas na transição contratual.	Não atende	Atende
	Permite maior segurança e controle dos dados.	Não atende	Atende
	Baixo risco de indisponibilidade de dados.	Atende	Atende
Tecnológico	Dispõe de garantia e suporte técnico especializado.	Atende	Atende
	Os itens que compõem a solução devem possuir compatibilidade tecnológica.	Atende	Atende
	Conhecimento técnico pré-existente no órgão.	Atende	Atende
	Permite o prolongamento da vida útil dos equipamentos (sobrevida) ou da solução adotada	Não atende	Atende
Resultado da Análise		Não atende plenamente	Atende plenamente

10. REGISTRO DE SOLUÇÕES CONSIDERADAS INVIÁVEIS

Solução 1: Contratação de serviço.

A EPC considera que esta solução, no atual contexto da Universidade Federal do Paraná, é inviável com base nos seguintes motivos:

- Riscos de descontinuidade contratual: os contratos de serviços continuados implicam em um maior risco de interrupção das atividades da Contratante, dado que o orçamento das IFES é sujeito a contingenciamentos recorrentes, que poderiam implicar na indisponibilidade dos equipamentos e softwares utilizados diariamente na Instituição para execução de diversas atividades essenciais.

- Por tratar-se de uma inovação no mercado brasileiro, em especial no ambiente público, a UFPR enfrentaria uma série de dificuldades para o planejamento e a implantação deste modelo de contratação. Embora esse tipo de contratação esteja ganhando força no setor privado, no serviço público são escassas as

iniciativas de sua adoção.
Dessa forma, a Solução 1 foi considerada inviável pelas desvantagens elencadas, restando apenas a Solução 2 como opção viável.

11. ANÁLISE COMPARATIVA DE CUSTOS (TCO)

O Custo Total de Propriedade (do inglês *Total Cost of Ownership* - TCO) é uma técnica de análise de custos que considera os custos inerentes ao ciclo de vida dos bens e serviços da solução.
Para a Solução 2 (única viável), além do custo de aquisição do ativo também é necessário levar em consideração sua depreciação. De acordo com as normas contábeis em vigor, a vida útil dos bens de informática é de 5 (cinco) anos, assim, ao fim desse período o ativo possuirá valor contábil residual da depreciação.

11.1. CÁLCULO DOS CUSTOS TOTAIS DE PROPRIEDADE (TCO)

Os cálculos na Tabela 5, a título de exemplificação, utilizam como referência os valores estimados para os componentes da solução, conforme valor de mercado dos equipamentos, softwares e serviços almejados.

Tabela 5 – Custos para Aquisição de Equipamentos

OBJETO	QUANTIDADE	VALOR UNITÁRIO	VALOR TOTAL
SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses.	2	R\$ 1.198.660,98	R\$ 2.397.321,96
SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses.	2	R\$ 491.754,86	R\$ 983.509,72
SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses.	2	R\$ 57.388,74	R\$ 114.777,48
PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses.	1100	R\$ 4.191,25	R\$ 4.610.375,00
PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses.	100	R\$ 6.897,81	R\$ 689.781,00
PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses.	20	R\$ 10.241,80	R\$ 204.836,00
CUSTO TOTAL ESTIMADO (COMPRA):			R\$ 9.000.601,16

A depreciação da solução considerando vida útil de 5 (cinco) anos, com taxa linear de 20% a.a., pode ser calculada conforme Tabela 6.

Tabela 6 – Depreciação dos Equipamentos

OBJETO	VALOR INICIAL	ANO 1	ANO 2	ANO 3	ANO 4	ANO 5
SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses.	R\$ 2.397.321,96	-R\$ 479.464,39	-R\$ 383.571,51	-R\$ 306.857,21	-R\$ 245.485,77	-R\$ 196.388,61
	Depreciação Acumulada	-R\$ 479.464,39	-R\$ 863.035,91	-R\$ 1.169.893,12	-R\$ 1.415.378,89	-R\$ 1.611.767,50
	Residual	R\$ 1.917.857,57	R\$ 1.534.286,05	R\$ 1.227.428,84	R\$ 981.943,07	R\$ 785.554,46
SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses.	R\$ 983.509,72	-R\$ 196.701,94	-R\$ 157.361,56	-R\$ 125.889,24	-R\$ 100.711,40	-R\$ 80.569,12
	Depreciação Acumulada	-R\$ 196.701,94	-R\$ 354.063,50	-R\$ 479.952,74	-R\$ 580.664,14	-R\$ 661.233,25
	Residual	R\$ 786.807,78	R\$ 629.446,22	R\$ 503.556,98	R\$ 402.845,58	R\$ 322.276,47
SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses.	R\$ 114.777,48	-R\$ 22.955,50	-R\$ 18.364,40	-R\$ 14.691,52	-R\$ 11.753,21	-R\$ 9.402,57
	Depreciação Acumulada	-R\$ 22.955,50	-R\$ 41.319,89	-R\$ 56.011,41	-R\$ 67.764,62	-R\$ 77.167,20
	Residual	R\$ 91.821,98	R\$ 73.457,59	R\$ 58.766,07	R\$ 47.012,86	R\$ 37.610,28
PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses.	R\$ 4.610.375,00	-R\$ 922.075,00	-R\$ 737.660,00	-R\$ 590.128,00	-R\$ 472.102,40	-R\$ 377.681,92
	Depreciação Acumulada	-R\$ 922.075,00	-R\$ 1.659.735,00	-R\$ 2.249.863,00	-R\$ 2.721.965,40	-R\$ 3.099.647,32
	Residual	R\$ 3.688.300,00	R\$ 2.950.640,00	R\$ 2.360.512,00	R\$ 1.888.409,60	R\$ 1.510.727,68
PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses.	R\$ 689.781,00	-R\$ 137.956,20	-R\$ 110.364,96	-R\$ 88.291,97	-R\$ 70.633,57	-R\$ 56.506,86
	Depreciação Acumulada	-R\$ 137.956,20	-R\$ 248.321,16	-R\$ 336.613,13	-R\$ 407.246,70	-R\$ 463.753,56
	Residual	R\$ 551.824,80	R\$ 441.459,84	R\$ 353.167,87	R\$ 282.534,30	R\$ 226.027,44
PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses.	R\$ 204.836,00	-R\$ 40.967,20	-R\$ 32.773,76	-R\$ 26.219,01	-R\$ 20.975,21	-R\$ 16.780,17
	Depreciação Acumulada	-R\$ 40.967,20	-R\$ 73.740,96	-R\$ 99.959,97	-R\$ 120.935,17	-R\$ 137.715,34
	Residual	R\$ 163.868,80	R\$ 131.095,04	R\$ 104.876,03	R\$ 83.900,83	R\$ 67.120,66

Em seguida, a Tabela 7 apresenta o cálculo do valor de aquisição dos demais itens que compõem a solução.

Tabela 7 – Custos para Aquisição de Softwares, Licenças, Serviços de Configuração e Peças

CLASSIFICAÇÃO	DESCRIÇÃO DOS ITENS	VALOR TOTAL DOS ITENS	VALOR TOTAL
	SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	R\$ 26.656,71	
	LICENÇAS PARA SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO) PARA 1.000 DISPOSITIVOS	R\$ 493.470,35	
	SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO	R\$ 10.518,56	
	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I (1.000 DISPOSITIVOS)	R\$ 151.655,35	

Softwares e Licenças	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II (10.000 DISPOSITIVOS)	R\$ 181.248,92	R\$ 2.146.622,72
	SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	R\$ 130.893,30	
	SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	R\$ 132.772,30	
	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO I (25GB/DIA)	R\$ 133.863,88	
	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO II (500GB/DIA)	R\$ 443.287,89	
	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL (ATÉ 10 FIREWALLS)	R\$ 5.716,28	
	SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES (LICENÇA DE 3 ANOS PARA 2.000 USUÁRIOS)	R\$ 436.539,18	
Peças (Injetores PoE e Transceivers)	INJETOR PoE (Power Injector)	R\$ 80.037,50	R\$ 314.027,90
	TRANSCEIVER 10GE SFP+ SR: Multimodo, LC Duplex, 300m.	R\$ 21.789,12	
	TRANSCEIVER 10GE SFP+ LR: Monomodo, LC Duplex, 10km.	R\$ 20.177,64	
	TRANSCEIVER 40GE QSFP+ SR: Multimodo, MPO, 150m.	R\$ 72.774,72	
	TRANSCEIVER 40GE QSFP+ LR: Monomodo, LC Duplex, 10km.	R\$ 119.248,92	
Serviços de Configuração	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO I	R\$ 50.378,14	R\$ 401.954,37
	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO II	R\$ 43.253,80	
	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO III	R\$ 30.396,84	
	SERVIÇO DE CONFIGURAÇÃO PARA LICENÇA DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	R\$ 23.487,30	
	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I	R\$ 23.487,30	
	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II	R\$ 36.964,40	
	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	R\$ 27.979,67	
	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	R\$ 32.472,04	
	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS	R\$ 18.994,94	
	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL	R\$ 23.487,30	
	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES	R\$ 91.052,64	
	CUSTO TOTAL ESTIMADO (COMPRA):		R\$ 2.862.604,99

Ao final, considerando o custo de aquisição, a perda acumulada por depreciação e o valor residual da solução, verifica-se o custo total de propriedade (TCO) na Tabela 8:

Tabela 8 – Custos Totais de Propriedade (TCO) da Contratação

OBJETO		VALOR TOTAL
SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses.	Custo Aquisição	R\$ 2.397.321,96
	Depreciação Acumulada	R\$ 1.611.767,50
	Valor Residual	-R\$ 785.554,46
SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses.	Custo Aquisição	R\$ 983.509,72
	Depreciação Acumulada	R\$ 661.233,25
	Valor Residual	-R\$ 322.276,47
SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses.	Custo Aquisição	R\$ 114.777,48
	Depreciação Acumulada	R\$ 77.167,20
	Valor Residual	-R\$ 37.610,28
PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses.	Custo Aquisição	R\$ 4.610.375,00
	Depreciação Acumulada	R\$ 3.099.647,32
	Valor Residual	-R\$ 1.510.727,68
PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses.	Custo Aquisição	R\$ 689.781,00
	Depreciação Acumulada	R\$ 463.753,56
	Valor Residual	-R\$ 226.027,44
PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses.	Custo Aquisição	R\$ 204.836,00
	Depreciação Acumulada	R\$ 137.715,34
	Valor Residual	-R\$ 67.120,66
Softwares e Licenças	Custo Aquisição	R\$ 2.146.622,72
Peças (Injetores PoE e Transceivers)	Custo Aquisição	R\$ 314.027,90
Serviços de Configuração	Custo Aquisição	R\$ 401.954,37
CUSTO TOTAL DE PROPRIEDADE ESTIMADO (com depreciação)		R\$ 14.965.173,33

11.2. MAPA COMPARATIVO DOS CÁLCULOS TOTAIS DE PROPRIEDADE (TCO)

Verificou-se apenas uma solução viável, portanto, não é possível a elaboração de um mapa comparativo com as soluções identificadas.

12. DESCRIÇÃO DA SOLUÇÃO DE TIC A SER CONTRATADA

Solução 2: Aquisição de equipamentos e softwares

A alternativa de aquisição de solução unificada de segurança e conectividade da UFPR se configura como a única opção viável, em razão de possibilitar o

crescimento gradativo e o atendimento de novas demandas, conforme a disponibilidade de recursos orçamentários. Além disso, a alternativa adota o modelo de serviço *on-premise* no qual todos os recursos da solução pertencem à Universidade e isso elimina o risco de indisponibilidade do serviço por questões financeiras de manutenção de contrato.

Adicionalmente, a contratação permitirá o atendimento das demandas da UFPR por segurança da informação e conectividade, favorecendo a redução de custos (ganho de economia de escala), a padronização do parque e dos serviços contratados, além da possibilidade de manter os equipamentos e softwares por período superior ao prazo de garantia.

13. ESTIMATIVA DE CUSTO TOTAL DA CONTRATAÇÃO

A Tabela 9 apresenta a estimativa de custo total da contratação, contendo a descrição, quantidade, valores unitários e totais para cada um dos itens.

Tabela 9 – Estimativa de Custo Total da Contratação

Lote	Item	Descrição	Quantidade	Métrica	Valor Unitário	Valor Total
	1	SOLUÇÃO DE FIREWALL TIPO I: Firewall de Borda Rede Externa (conexão externa de internet), com garantia de 60 meses.	2	Unidade	R\$ 1.198.660,98	R\$ 2.397.321,96
	2	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO I	2	Unidade	R\$ 25.189,07	R\$ 50.378,14
	3	SOLUÇÃO DE FIREWALL TIPO II: Firewall para Rede Interna (DMZ), com garantia de 60 meses.	2	Unidade	R\$ 491.754,86	R\$ 983.509,72
	4	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO II	2	Unidade	R\$ 21.626,90	R\$ 43.253,80
	5	SOLUÇÃO DE FIREWALL TIPO III: Firewall para Datacenters Descentralizados (fora da sede), com garantia de 60 meses.	2	Unidade	R\$ 57.388,74	R\$ 114.777,48
	6	SERVIÇO DE CONFIGURAÇÃO PARA SOLUÇÃO DE FIREWALL TIPO III	2	Unidade	R\$ 15.198,42	R\$ 30.396,84
	7	PONTO DE ACESSO INDOOR I: Access Point Interno 2x2, com garantia de 36 meses.	1.100	Unidade	R\$ 4.191,25	R\$ 4.610.375,00
	8	PONTO DE ACESSO INDOOR II: Access Point Interno 4x4 (alta densidade), com garantia de 36 meses.	100	Unidade	R\$ 6.897,81	R\$ 689.781,00
	9	PONTO DE ACESSO OUTDOOR: Access Point Externo, com garantia de 36 meses.	20	Unidade	R\$ 10.241,80	R\$ 204.836,00
	10	INJETOR PoE (Power Injector)	50	Unidade	R\$ 1.600,75	R\$ 80.037,50
	11	SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	1	Unidade	R\$ 26.656,71	R\$ 26.656,71
	12	LICENÇAS PARA SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO) PARA 1.000 DISPOSITIVOS	5	Unidade	R\$ 98.694,07	R\$ 493.470,35
	13	SERVIÇO DE CONFIGURAÇÃO PARA LICENÇA DE SOLUÇÃO DE CONTROLE DE ACESSO À REDE (PERÍMETRO)	1	Unidade	R\$ 23.487,30	R\$ 23.487,30
	14	SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO	1	Unidade	R\$ 10.518,56	R\$ 10.518,56
	15	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I (1.000 DISPOSITIVOS)	5	Unidade	R\$ 30.331,07	R\$ 151.655,35

16	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO I	1	Unidade	R\$ 23.487,30	R\$ 23.487,30
17	LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II (10.000 DISPOSITIVOS)	1	Unidade	R\$ 181.248,92	R\$ 181.248,92
18	SERVIÇO DE CONFIGURAÇÃO DE LICENÇAS PARA SOLUÇÃO DE GERENCIAMENTO DE IDENTIDADE E ACESSO TIPO II	1	Unidade	R\$ 36.964,40	R\$ 36.964,40
19	SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	1	Unidade	R\$ 130.893,30	R\$ 130.893,30
20	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE PROTEÇÃO DE E-MAIL COM RECURSOS AVANÇADOS, INCLUINDO A ANÁLISE DE URL E ARQUIVOS DE SANDBOX	1	Unidade	R\$ 27.979,67	R\$ 27.979,67
21	SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	2	Unidade	R\$ 66.386,15	R\$ 132.772,30
22	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE GERENCIAMENTO DE ACESSO PRIVILEGIADO LOCAL (PAM)	1	Unidade	R\$ 32.472,04	R\$ 32.472,04
23	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO I (25GB/DIA)	2	Unidade	R\$ 66.931,94	R\$ 133.863,88
24	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS TIPO II (500GB/DIA)	1	Unidade	R\$ 443.287,89	R\$ 443.287,89
25	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE LOGS	1	Unidade	R\$ 18.994,94	R\$ 18.994,94
26	PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL (ATÉ 10 FIREWALLS)	1	Unidade	R\$ 5.716,28	R\$ 5.716,28
27	SERVIÇO DE CONFIGURAÇÃO DE PLATAFORMA DE GERÊNCIA CENTRALIZADA DE FIREWALL	1	Unidade	R\$ 23.487,30	R\$ 23.487,30
28	SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES (LICENÇA DE 3 ANOS PARA 2.000 USUÁRIOS)	3	Unidade	R\$ 145.513,06	R\$ 436.539,18
29	SERVIÇO DE CONFIGURAÇÃO DE SOLUÇÃO DE IDENTIFICAÇÃO E AUTENTICAÇÃO DE ACESSO DE VISITANTES	3	Unidade	R\$ 30.350,88	R\$ 91.052,64
30	TRANSCEIVER 10GE SFP+ SR: Multimodo, LC Duplex, 300m.	24	Unidade	R\$ 907,88	R\$ 21.789,12
31	TRANSCEIVER 10GE SFP+ LR: Monomodo, LC Duplex, 10km.	12	Unidade	R\$ 1.681,47	R\$ 20.177,64
32	TRANSCEIVER 40GE QSFP+ SR: Multimodo, MPO, 150m.	16	Unidade	R\$ 4.548,42	R\$ 72.774,72
33	TRANSCEIVER 40GE QSFP+ LR: Monomodo, LC Duplex, 10km.	6	Unidade	R\$ 19.874,82	R\$ 119.248,92
Custo Estimado da Contratação:					R\$ 11.863.206,15

Custo estimado da Contratação: **R\$ 11.863.206,15 (onze milhões oitocentos e sessenta e três mil duzentos e seis reais e quinze centavos).**

14. JUSTIFICATIVA TÉCNICA DA ESCOLHA DA SOLUÇÃO

Do ponto de vista técnico, a aquisição de equipamentos e softwares com as garantias especificadas assegura o atendimento pleno dos requisitos técnicos necessários para melhor aproveitamento da solução.

Destaque-se os seguintes aspectos técnicos:

- Aproveitamento do conhecimento técnico já adquirido na gestão da solução de Next Generation Firewall do fabricante Fortinet, uma vez que os demais componentes agregados na presente contratação utilizam a mesma (lógica de) interface de gerenciamento.
- A análise centralizada de logs de auditoria de todos os componentes da solução, permitindo a identificação mais eficiente e efetiva da ameaça.
- A adição de camada de segurança na gestão de vulnerabilidades providas da rede wi-fi, a qual possui a maior superfície de ataque na UFPR, dada sua abrangência.
- O ganho de performance, da capacidade e o aumento da cobertura da rede wi-fi somente possíveis com a ampliação e modernização do parque de access points.
- O fato de que a solução de antenas (access points) do fabricante Fortinet não necessitam de licenças para operar.
- O maior controle das redes, que poderão filtrar e controlar quais dispositivos ou usuários se conectam à rede, permitindo que sejam automaticamente direcionados para a rede apropriada (segmentação de rede) baseado em políticas de segurança.
- O suporte controlado por ferramentas especializadas no permissionamento de usuários com privilégios elevados.
- A adição de uma camada extra, avançada e em tempo real no controle de *phishing* e outros malwares na solução de e-mail do Microsoft 365, sobretudo capazes de reduzir a invasão de contas de usuários, um problema recorrente e de difícil gestão sem ferramentas apropriadas.
- O adequado nível de controle de acesso ao prover identificação e autenticação de visitantes nas redes internas, hoje não disponíveis de maneira segura (as redes para eventos são disponibilizadas com senha única e não se conhece a identidade do ingressante).

14.1. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS TÉCNICOS

A contratação prevê o agrupamento em função de aspectos técnicos da solução de TIC a ser contratada. O Lote 1 (lote único) é composto por equipamentos como firewall, access points, softwares, licenças, serviços, entre outros. Esse agrupamento é o mais adequado, caso contrário o parcelamento da solução, que teria como pressuposto a intenção de que vários fornecedores pudessem atender a UFPR, não se mostra gerencialmente e tecnicamente viável. Nessa abordagem, cada componente da solução, incluindo os serviços de garantia e suporte técnico, estaria sujeito à atuação conjunta de mais de um fornecedor, incluindo a oferta de equipamentos de diversas marcas e modelos, aumentando os riscos da contratação causados pela complexidade e problemas de compatibilidade dos equipamentos e softwares.

Dessa forma, os itens que integram o Lote 1 da presente contratação precisam ser totalmente compatíveis entre si, provendo a perfeita interoperabilidade da solução. O fornecimento de tais itens por diversos fabricantes acarretaria na impossibilidade de integração, de modo que os requisitos e necessidades não seriam atendidos, impedindo atingimento dos objetivos.

O parcelamento do Lote 1 em diversos itens pode acarretar prejuízos quanto à instalação, configuração e operacionalização de toda a solução, bem como sua manutenção, uma vez que se exige total compatibilidade entre os equipamentos e softwares a serem adquiridos. Além disso, a definição do agrupamento impacta na redução de custos operacionais, na capacidade técnica de manter a solução em operação, nos recursos humanos disponíveis para prestarem o devido apoio, curva de aprendizagem e no custo total de propriedade.

14.2. UTILIZAÇÃO DO CATÁLOGO ELETRÔNICO DE PADRONIZAÇÃO E CATÁLOGO DE SOLUÇÕES DE TIC

Conforme estabelecido no art. 40, §1º, inciso I, da Lei nº 14.133, de 2021, e o art. 9º, inciso I, alínea b, da Instrução Normativa Seges/ME nº 81, de 2022, deve ser feita a especificação do produto/bem/serviço, preferencialmente conforme catálogo eletrônico de padronização, observados os requisitos de qualidade, rendimento, compatibilidade, durabilidade e segurança. Nesse sentido, foi realizada uma consulta ao Catálogo Eletrônico de Padronização e verificou-se que a presente contratação não está contemplada em seus termos.

No que diz respeito aos softwares e suas respectivas licenças foram realizadas consultas no Catálogo de Soluções de TIC com Condições Padronizadas, porém também não foram encontrados códigos PMC-TIC com a identificação dos softwares pretendidos.

15. JUSTIFICATIVA ECONÔMICA DA ESCOLHA DA SOLUÇÃO

Do ponto de vista econômico, foram avaliadas as soluções disponíveis no mercado e em outros órgãos e após análise das soluções, suas vantagens, desvantagens e custos totais de propriedade, a escolha da **Solução 2** (única opção viável) é justificada por apresentar os aspectos que visam garantir maior eficácia, eficiência, efetividade e economicidade à contratação.

15.1. DO PARCELAMENTO DA CONTRATAÇÃO DECORRENTE DE ASPECTOS ECONÔMICOS

Após as análises realizadas, conclui-se que a adjudicação por lote único, além de respeitar as regulamentações e recomendações pertinentes, demonstrou ser a opção mais vantajosa para a Administração Pública. Ademais, existem vários fornecedores no mercado com plena capacidade de ofertar a solução almejada, proporcionando economicidade e atendendo aos princípios da competitividade e da isonomia.

16. BENEFÍCIOS A SEREM ALCANÇADOS COM A CONTRATAÇÃO

Ao investir em uma solução de segurança da informação nativamente integrada e associada com a rede de dados sem fio da Universidade Federal do Paraná, com os componentes incluídos na presente contratação (firewall de nova geração para proteção de borda, pontos de acesso WLAN, controle de acesso seguro à rede, controle de acesso privilegiado, gerenciamento de identidade, proteção de e-mail, identificação e autenticação de acesso de visitantes e gestão centralizada de logs de auditoria), vários resultados positivos podem ser esperados. Abaixo a EPC lista os principais benefícios:

- Aumento da maturidade institucional em segurança da informação de acordo com as medições do PPSI ao investir em medidas consideradas prioritárias pelo referido Programa.
- Facilitação da gestão da segurança da informação e aumento da visibilidade das ameaças cibernéticas, incluindo condições de rastreamento dos pontos de vulnerabilidade.
- Proteção robusta e contínua com detecção e bloqueio contra ameaças avançadas providas da Internet via firewall de nova geração (NGFW), uma vez que oferece defesa aprimorada contra malwares, ataques de negação de serviço (DDoS), explorações *zero-day* e outras ameaças cibernéticas sofisticadas.
- Controle granular de aplicações e de usuários via Firewall, no qual pode-se implementar políticas detalhadas de controle de acesso, permitindo ou bloqueando o uso de aplicações específicas com base em usuários, grupos ou dispositivos, melhorando a segurança e otimizando o uso dos recursos.
- Maior garantia de segurança para dispositivos móveis e remotos com os recursos de VPN e controles de acesso remoto incluídos no Firewall, possibilitando que a Universidade garanta que alunos, professores e demais colaboradores possam acessar a rede de forma segura, mesmo em ambientes externos, como em casa ou durante viagens.
- Segurança aprimorada no acesso à rede com NAT (*Network Address Translation*) e gerenciamento de identidade, com os quais a universidade poderá garantir que apenas dispositivos e usuários autorizados tenham acesso aos recursos, minimizando vulnerabilidades.
- Segmentação e isolamento de redes, uma vez que firewall + NAT permitirão segmentação eficiente das redes internas, isolando áreas críticas (como o datacenter, redes administrativas e laboratórios de pesquisa) de áreas comuns (como rede de visitantes e de acesso por alunos), reduzindo a superfície de ataque interno e invasão.
- Gerenciamento centralizado e simplificado com a integração dos diversos componentes em uma plataforma unificada, que permitirá um controle mais eficiente de todos os aspectos da segurança, com visibilidade consolidada e gestão de logs centralizada.

- Maior controle sobre acessos privilegiados, que proporcionará mais segurança na administração de usuários com permissões elevadas, reduzindo o risco de ataques internos.
- Proteção avançada de e-mails para filtragem de mensagens maliciosas, *phishing* e spams, fortalecendo a segurança das comunicações corporativas e reduzindo a níveis aceitáveis e gerenciáveis as contas comprometidas, protegendo os alunos, professores e demais colaboradores de golpes e de roubo de dados pessoais.
- Redução de riscos associados a visitantes com a solução de identificação e autenticação de visitantes, que garantirá que o acesso à rede por terceiros seja devidamente controlado e auditado, melhorando a segurança dos frequentes eventos e visitas promovidos na Universidade.
- Aumento da eficiência operacional com a integração nativa entre a rede sem fio (WLAN) e os outros componentes de segurança, com consequente simplificação da administração e do monitoramento, resultando em menos interrupções e uma infraestrutura mais estável e confiável.
- Respostas mais rápidas a incidentes com a gestão centralizada de logs de auditoria, que permitirá uma análise mais rápida e precisa de eventos de segurança, ajudando a identificar e mitigar incidentes com maior velocidade.
- Conformidade regulatória/legal facilitada, dado que a solução ajudará a Universidade a cumprir normas de segurança (incluindo a POSIC) e privacidade (como LGPD), oferecendo controle detalhado de acessos e atividades, além de relatórios de conformidade.
- Otimização de recursos de TI, pois a centralização da segurança em uma solução integrada reduz a complexidade operacional para a equipe de TI da Universidade, diminuindo o tempo gasto com múltiplas ferramentas e melhorando a capacidade de resposta a incidentes.
- Redução de custos a longo prazo, pois, embora o investimento inicial possa ser significativo, uma solução de segurança integrada pode reduzir os custos a longo prazo ao minimizar incidentes de segurança com ou sem vazamento de dados, evitar multas por não conformidade e diminuir a necessidade de correções emergenciais, além de reduzir a necessidade de várias soluções independentes.
- Melhor performance da rede sem fio integrada à infraestrutura de segurança, com otimização do desempenho da rede, proporcionando conectividade estável e segura para alunos, convidados e colaboradores.
- Prevenção de acessos não autorizados com o controle de identidade e autenticação robustos e confiáveis, garantindo que apenas usuários autenticados tenham acesso a serviços e sistemas, prevenindo acessos não autorizados.
- Melhoria na visibilidade e monitoramento de tráfego, dado que a integração de soluções de segurança proporcionará visibilidade abrangente sobre o tráfego da rede, permitindo detectar e reagir rapidamente a atividades suspeitas.

Esses benefícios fortalecerão a postura de segurança da Universidade Federal do Paraná, protegendo suas operações acadêmicas e administrativas.

17. PROVIDÊNCIAS A SEREM ADOTADAS

Necessidade	Responsável(is)	Envolvido(s)
Levantamento e adequação das necessidades de infraestrutura de rede lógica e elétrica nos espaços físicos dos locais onde os equipamentos serão instalados, tais como: postes, canaletas, eletrocalhas, cabos, conectores, <i>patch panel</i> e qualquer outro material de infraestrutura que deva ser provido pela UFPR.	AGTIC	CSI
Disponibilização de portas em switches (requer fornecimento de equipamentos switches em rede de dados estruturada).	AGTIC	CSI
Prover a infraestrutura de datacenter necessária para instalação da solução, disponibilizando capacidade de processamento, memória e espaço em disco, conforme especificações do fabricante.	AGTIC	CSI
Revisão dos links de fibra ótica para suportar velocidades de transmissão mais altas.	AGTIC	CSI

18. CONTRATAÇÕES CORRELATAS E OU INTERDEPENDENTES

Não foram identificadas outras contratações correlatas ou interdependentes necessárias para o presente objeto.

19. DECLARAÇÃO DE VIABILIDADE

19.1. JUSTIFICATIVA

A declaração da viabilidade da contratação expressa nesta seção apresenta a justificativa da solução escolhida, abrangendo a identificação dos benefícios a serem alcançados em termos de eficácia, eficiência, efetividade e economicidade.

Nesse sentido, identificou-se no estudo que a solução incorpora:

- Eficácia, ao atender de forma abrangente e unificada as diversas necessidades de serviços de segurança e conectividade, especialmente nos aspectos de disponibilidade, confiabilidade, integridade e autenticidade para os dados armazenados no datacenter ou em tráfego em suas redes.
- Efetividade, ao atender os requisitos técnicos e de negócio da UFPR com os prazos e recursos orçamentários disponíveis e totalmente alinhados com o framework do PPSI.
- Eficiência, ao atingir um alto nível de serviço com a redução de complexidade, com a utilização de soluções especializadas e tecnologicamente atuais, com integração nativa e devidamente cobertas por garantia e suporte técnico do fabricante.
- Economicidade, ao possibilitar o alcance dos resultados desejados com a melhor relação entre custo e benefício quando comparado às demais soluções não unificadas identificadas, além de reduzir os custos a longo prazo ao minimizar incidentes de segurança com ou sem vazamento de dados, evitar multas por não conformidade e diminuir a necessidade de correções emergenciais, além de reduzir a necessidade de várias soluções independentes.

Ressalte-se que a área de Segurança da Informação permeia todos os elementos que envolvem os dados, sejam eles humanos, tecnológicos ou processuais. Dessa forma, uma gestão eficaz de segurança necessita que todos os componentes sejam finamente integráveis, de forma que as medidas de segurança e as informações de um componente possam complementar os outros, provendo controle efetivo das ameaças ou possibilitando seu rastreo e as vulnerabilidades exploradas. Por sua vez, ao integrar redes de conectividade sem fio à solução de segurança do mesmo fabricante cujo foco é Segurança da Informação, obtém-se um maior controle da rede que, por sua vez, atualmente é o canal mais vulnerável para a entrada de ameaças na UFPR, visto que seu uso se dá por um contingente muito amplo de usuários.

Considerando as informações do presente estudo, entende-se que a contratação se configura tecnicamente VIÁVEL, sendo relevante e essencial para o desenvolvimento das atividades de ensino, pesquisa, extensão e inovação da UFPR.

20. RESPONSÁVEIS

A Equipe de Planejamento da Contratação foi instituída pela Portaria nº 227/2024-CLIC (7167384), de 16 de outubro de 2024.

Conforme o § 2º do Art. 11 da IN SGD/ME nº 94/2022, o Estudo Técnico Preliminar da Contratação será aprovado e assinado pelos Integrantes Técnico e Requisitante da Equipe de Planejamento da Contratação e pela autoridade máxima da Área de TIC.

INTEGRANTE TÉCNICO	INTEGRANTE REQUISITANTE
Giovanni Allam Taborda Analista de Tecnologia da Informação Matrícula/SIAPE: 2909475 Valmir Antunes Pereira Gestor de Segurança da Informação Matrícula/SIAPE: 1526015	Gustavo de Brito dos Santos Coordenador da Coordenadoria de Serviços e Infraestrutura de TIC (CSI) Matrícula/SIAPE: 1111747

21. APROVAÇÃO E DECLARAÇÃO DE CONFORMIDADE

Aprovo este Estudo Técnico Preliminar e atesto sua conformidade às disposições da Instrução Normativa SGD/ME nº 94, de 23 de dezembro de 2022.

AUTORIDADE MÁXIMA DA ÁREA DE TIC
Felipe Sanches Bueno Diretor Executivo da AGTIC Matrícula/SIAPE: 1653832

ANEXO III - MINUTA DE ATA DE REGISTRO DE PREÇOS
PREGÃO ELETRÔNICO Nº 90.002/2025

(Este documento foi elaborado com base no modelo da AGU de maio de 2023)
As partes redigidas em preto seguem conforme modelo estabelecido pela AGU e recomenda-se serem mantidas.
Para as partes redigidas em vermelho, teremos 2 situações:
1 - As que deverão ser preenchidas conforme a natureza do objeto a ser contratado;
2 - E as que necessitarão ser avaliadas conforme a natureza do objeto, podendo ser suprimidas nos casos em que a redação não seja aplicável
As partes destacadas em amarelo se referem a alterações ou complementos realizados por esta UASG que não estavam previstos no modelo da AGU

UNIVERSIDADE FEDERAL DO PARANÁ (153079)
ATA DE REGISTRO DE PREÇOS
ATA N.º XX/20XX

A UNIVERSIDADE FEDERAL DO PARANÁ, com sede à Rua XV de Novembro, nº 1299, na cidade de Curitiba /Estado do Paraná, inscrita no CNPJ sob o nº 75.095.679/0001-49, neste ato representado(a) pelo(a) Pró-Reitor de Administração, NOME COMPLETO, conforme delegação de competência pela Portaria nº XXX, de DD/MM/AAAA, do Magnífico Reitor, Portaria nº de de de 20..., publicada no DOU de de de, portador da Matrícula Funcional nº, considerando o julgamento da licitação na modalidade de pregão, na forma eletrônica, para REGISTRO DE PREÇOS nº/202..., publicada no de/202..., processo administrativo n.º 23075.049214/2024-91, 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 Pregão Eletrônico nº 90.002/2025, sujeitando-se as partes às normas constantes na Lei nº 14.133, de 1º de abril de 2021, no Decreto n.º 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 solução unificada de segurança e conectividade, especificado(s) no(s) item(ns)..... do Termo de Referência, anexo I do Edital de Pregão Eletrônico nº 90.002/2025, 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 mínimas e máximas de cada item, fornecedor(es) e as demais condições ofertadas na(s) proposta(s) são as que seguem:

Item do TR	Fornecedor (razão social, CNPJ/MF, endereço, contatos, representante)					
X	Especificação	Marca e modelo	Unidade	Quantidade	Valor Un	Prazo garantia ou validade
	Descrição do Item no Edital		Unidade prevista no edital			

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 a Universidade Federal do Paraná (UASG 153079).
3.2 {Além do gerenciador, não há [ou] São} órgãos e entidades públicas participantes do registro de preços:

Item nº	Órgãos Participantes	Unidade	Quantidade

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:

- a) apresentação de justificativa da vantagem da adesão, inclusive em situações de provável desabastecimento ou descontinuidade de serviço público;
- b) 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
- c) 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 a 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 Para aquisição emergencial de medicamentos e material de consumo médico-hospitalar por órgãos e entidades da Administração Pública federal, estadual, distrital e municipal, a adesão à ata de registro de preços gerenciada pelo Ministério da Saúde não estará sujeita ao limite previsto no item 4.7.

4.9 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

4.10 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.

5.2 A contratação com os fornecedores registrados na ata será formalizada pelo órgão ou pela entidade interessada por intermédio de emissão de nota de empenho de despesa, conforme o art. 95 da Lei nº 14.133, de 2021.

5.3 Após a homologação da licitação ou da contratação direta, deverão ser observadas as seguintes condições para formalização da ata de registro de preços:

5.3.1 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 Termo de Referência e se obrigar nos limites dela;

5.3.2 Será incluído na ata, na forma de anexo, o registro dos licitantes ou dos fornecedores que:

- a) Aceitarem cotar os bens, as obras ou os serviços com preços iguais aos do adjudicatário, observada a classificação da licitação; e
- b) Mantiverem sua proposta original.

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

5.4 O registro a que se refere o item 5.3.2 tem por objetivo a formação de cadastro de reserva para o caso de impossibilidade de atendimento pelo signatário da ata.

5.5 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.

5.6 A habilitação dos licitantes que comporão o cadastro de reserva a que se refere a alínea "b)" do item 5.3.2 somente será efetuada quando houver necessidade de contratação dos licitantes remanescentes, nas seguintes hipóteses:

- a) Quando o licitante vencedor não assinar a ata de registro de preços, no prazo e nas condições estabelecidos no edital; e
- b) Quando houver o cancelamento do registro do licitante ou do registro de preços nas hipóteses previstas no item 9.

5.7 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.

5.8 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.

5.8.1 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.

5.9 A ata de registro de preços será assinada por meio de assinatura digital e disponibilizada no Sistema de Registro de Preços.

5.10 Quando o convocado não assinar a ata de registro de preços no prazo e nas condições estabelecidos no edital, e observado o disposto no item 5.8 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.

5.11 Na hipótese de nenhum dos licitantes que trata a alínea "a)" do item 5.3.2, aceitar a contratação nos termos do item anterior, a Administração, observados o valor estimado e sua eventual atualização nos termos do edital, poderá:

- a) 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
- b) Adjudicar e firmar o contrato nas condições ofertadas pelos licitantes ou fornecedores remanescentes, atendida a ordem classificatória, quando frustrada a negociação de melhor condição.
- 5.12 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:

- a) 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;
- b) 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;
- c) 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.
- i. No caso do reajustamento, deverá ser respeitada a contagem da anualidade e o índice previstos para a contratação;
 - ii. 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 diligenciarem negociação com vistas à alteração contratual, observado o disposto no art. 124 da Lei nº 14.133, de 2021.

7.2 Na hipótese de o preço de mercado tornar-se superior ao preço registrado e o fornecedor não poder cumprir as obrigações estabelecidas na ata, será facultado ao fornecedor requerer ao gerenciador a alteração do preço registrado, mediante comprovação de fato superveniente que supostamente o impossibilite de cumprir o compromisso.

7.2.1 Neste caso, o fornecedor encaminhará, juntamente com o pedido de alteração, a documentação comprobatória e a planilha de custos que demonstre a **inexequibilidade** do preço registrado em relação às condições inicialmente pactuadas.

7.2.2 O requerimento deverá ser entregue diretamente à Unidade de Contratos da Coordenadoria de Licitações e Contratações, através do e-mail contratos@ufpr.br.

7.2.3 Na hipótese de não comprovação da existência de fato superveniente que inviabilize o preço registrado, o pedido será indeferido pelo órgão ou entidade gerenciadora e o fornecedor deverá cumprir as obrigações estabelecidas na ata, sob pena de cancelamento do seu registro, nos termos do item 9.1, sem prejuízo das sanções previstas na Lei nº 14.133, de 2021, e na legislação aplicável.

7.2.4 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.

7.3 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.

7.4 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.

7.5 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.

7.6 O fornecedor fica obrigado a entregar, pelo preço registrado, os itens constantes das notas de empenho emitidas anteriormente a seu protocolo de solicitação de Alteração de Preços. Caso se recuse, estará sujeito às sanções descritas no Termo de Referência.

8. DA SUBSTITUIÇÃO DE PRODUTO

8.1 Durante a vigência desta ata de registro de preços, nas situações de impossibilidade de fornecimento de equipamentos registrados, devido à descontinuidade de produção ou outro motivo que impeça o fornecimento da marca e modelo do produto registrado, por prazo indeterminado, o fornecedor poderá apresentar à Unidade de Contratos da Coordenadoria de Licitações e Contratações, pedido para substituição de marca e/ou modelo do produto registrado.

8.1.1 Para aos bens de consumo duráveis, assim entendidos aqueles classificados pela UFPR como materiais permanentes, deverá ser realizada a substituição, preferencialmente, pelo modelo subsequente na linha de produção do mesmo fabricante, ou demonstrada sua inadequação aos termos do Edital da Licitação, conforme o caso.

8.2 Os pedidos de que trata o item 8.1 deverão conter:

- a) Comprovação emitida pelo fabricante, distribuidor, importador, representante ou equivalente, quanto à efetiva retirada do equipamento de linha ou dos motivos que impossibilitam o fornecimento;
- b) Catálogo, folheto técnico ou indicação do site do fornecedor, conforme previsão do anexo B do Termo de Referência, do produto substituto;

8.3 A análise de admissibilidade dos pedidos de substituição de produto será realizada pela Unidade de Contratos da Coordenadoria de Licitações e Contratações.

8.4 Uma vez acolhida a solicitação, a Unidade de Contratos da Coordenadoria de Licitações e Contratações poderá submeter o pedido à Unidade Gerenciadora da Ata no âmbito da UFPR, para a análise técnica do produto ofertado em substituição.

8.4.1 A análise da substituição levará em consideração o interesse público envolvido e ocorrerá observando o mesmo procedimento realizado no momento da análise técnica da licitação, ou seja, o equipamento substituto deverá atender todas as características do edital, bem como possuir qualidade igual ou superior a do equipamento ofertado na proposta original da licitação, vedado o aumento de preços.

8.5 Após a análise técnica o processo será enviado à Coordenadoria de Licitações e Contratações, que poderá acatar o pedido ou recusá-lo, liberando o fornecedor do compromisso assumido, se comprovada a inviabilidade de substituição.

8.6 Caso o pedido seja recusado, os itens solicitados mediante nota de empenho deverão ser entregues no prazo inicialmente estipulado, sob pena de aplicação das penalidades cabíveis.

9. REMANEJAMENTO DAS QUANTIDADES REGISTRADAS NA ATA DE REGISTRO DE PREÇOS

9.1 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.

9.2 O remanejamento somente poderá ser feito:

- a) De órgão ou entidade participante para órgão ou entidade participante; ou
- b) De órgão ou entidade participante para órgão ou entidade não participante.

9.3 O órgão ou entidade gerenciadora que tiver estimado as quantidades que pretende contratar será considerado participante para efeito do remanejamento.

9.4 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.

9.5 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.

9.6 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.

9.7 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 9.3, a distribuição das quantidades para a execução descentralizada será por meio do remanejamento.

10. CANCELAMENTO DO REGISTRO DO LICITANTE VENCEDOR E DOS PREÇOS REGISTRADOS

10.1 O registro do fornecedor será cancelado pelo gerenciador, quando o fornecedor:

- a) Descumprir as condições da ata de registro de preços, sem motivo justificado;
- b) Não retirar a nota de empenho, ou instrumento equivalente, no prazo estabelecido pela Administração sem justificativa razoável;
- c) Não aceitar manter seu preço registrado, na hipótese prevista no artigo 27, § 2º, do Decreto nº 11.462, de 2023; ou
- d) Sofrer sanção prevista nos incisos III ou IV do caput do art. 156 da Lei nº 14.133, de 2021.

10.1.1 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 poderá, mediante decisão fundamentada, decidir pela manutenção do registro de preços, vedadas contratações derivadas da ata enquanto perdurarem os efeitos da sanção.

10.2 O cancelamento de registros nas hipóteses previstas no item 10.1 será formalizado por despacho do órgão ou da entidade gerenciadora, garantidos os princípios do contraditório e da ampla defesa.

10.3 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.

10.4 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:

- a) Por razão de interesse público;
- b) A pedido do fornecedor, decorrente de caso fortuito ou força maior; ou
- c) Se não houver êxito nas negociações, nas hipóteses em que o preço de mercado tornar-se superior ou inferior ao preço registrado, nos termos dos artigos 26, § 3º e 27, § 4º, ambos do Decreto nº 11.462, de 2023.

11. DAS PENALIDADES

11.1 O descumprimento da Ata de Registro de Preços ensejará aplicação das penalidades estabelecidas no Termo de Referência.

11.1.1 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.

11.2 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).

11.3 O órgão ou entidade participante deverá comunicar ao órgão gerenciador qualquer das ocorrências previstas no item 10.1, dada a necessidade de instauração de procedimento para cancelamento do registro do fornecedor.

12. CONDIÇÕES GERAIS

12.1 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.

12.2 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.

12.3 Para firmeza e validade do pactuado, a presente Ata é assinada eletronicamente.

Local e data

Assinaturas

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

**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 e modelo	Unidade	Quantidade	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 e modelo	Unidade	Quantidade	Valor Un	Prazo garantia ou validade

**ANEXO IV
MINUTA DE CONTRATO**

(Este documento foi elaborado com base no modelo da AGU de **maio de 2023**)

A parte redigida em preto segue conforme modelo estabelecido pela AGU e recomenda-se serem mantidas.

As partes redigidas em vermelho preveem 2 situações:

1 - As que deverão ser preenchidas conforme a natureza do objeto a ser contratada,

2 - E as que necessitarão ser avaliadas conforme a natureza do objeto, podendo ser suprimidas nos casos em que a redação não seja aplicável

As partes destacadas em amarelo se referem a alterações ou complementos realizados por esta UASG que não estava previstos no modelo da AGU

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

A **UNIVERSIDADE FEDERAL DO PARANÁ**, com sede à Rua XV de Novembro, nº 1299, na cidade de Curitiba /Estado do Paraná, inscrita no CNPJ sob o nº 75.095.679/0001-49, neste ato representado(a) pelo(a) Pró-Reitor de Administração, NOME COMPLETO, conforme delegação de competência pela Portaria nº XXX, de DD/MM/AAAA, do Magnífico Reitor Portaria nº, de de.....de 20..., publicada no *DOU* de de.....de....., portador da Matrícula Funcional nº, doravante denominado CONTRATANTE, e por outro lado a Empresa o(a).....,inscrito(a) no CNPJ/MF sob o nº , sediado(a) na....., 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 nº. .../...*, mediante as cláusulas e condições a seguir enunciadas.

CLÁUSULA PRIMEIRA – OBJETO

1.1 Contratação de solução unificada de segurança e conectividade, nas condições estabelecidas no Termo de Referência.

1.2 Objeto da contratação:

Item	Descrição	CATMAT CATSER	Quantidade	Unidade de medida	Valor unitário	Valor total
1						
2						
3						
Valor Total da Contratação						

1.3 Vinculam esta contratação, independentemente de transcrição:

1.3.1 O Termo de Referência;

1.3.2 O Edital da Licitação;

1.3.3 A Proposta do contratado;

1.3.4 Eventuais anexos dos documentos supracitados.

CLÁUSULA SEGUNDA – VIGÊNCIA E PRORROGAÇÃO

2.1 **Para a aquisição de equipamentos** (itens 1, 3, 5, 30, 31, 32 e 33), deverá ser firmado contrato com prazo de vigência de 60 (sessenta) meses, contados da assinatura do contrato, visando garantir os requisitos de manutenção previstos no título 4.4 deste termo de referência, na forma do artigo 106 da Lei nº 14.133, de 2021.

OU

2.1 **Para a aquisição de equipamentos** (itens 7, 8, 9 e 10), deverá ser firmado contrato com prazo de vigência de 36 (trinta e seis) meses, contados da assinatura do contrato, visando garantir os requisitos de manutenção previstos no título 4.4 deste termo de referência, na forma do artigo 106 da Lei nº 14.133, de 2021.

OU

2.1 **Para a solução de softwares e licenças** (itens 11, 12, 14, 15, 17, 19, 21, 23, 24, 26 e 28), deverá ser firmado contrato com vigência de 36 (trinta e seis) meses), prorrogáveis por até 120 (cento e vinte) meses, na forma dos artigos 106 e 107 da Lei nº 14.133, de 2021, visando garantir os requisitos de manutenção previstos no título 4.4 deste termo de referência e a renovação das licenças adquiridas.

2.1.1 A prorrogação de que trata esse item é condicionada à avaliação, por parte do Gestor do Contrato, da vantajosidade da prorrogação, a qual deverá ser realizada motivadamente, com base no Histórico de Gestão do Contrato, nos princípios da manutenção da necessidade, economicidade e oportunidade da contratação, e nos demais aspectos que forem julgados relevantes.

2.2 O contratado não tem direito subjetivo à prorrogação contratual.

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

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

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

CLÁUSULA TERCEIRA – MODELOS DE EXECUÇÃO E GESTÃO CONTRATUAIS

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

CLÁUSULA QUARTA – SUBCONTRATAÇÃO

4.1 Não será admitida a subcontratação do objeto contratual.

CLÁUSULA QUINTA - PREÇO

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

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

5.3 O valor acima é meramente estimativo, de forma que os pagamentos devidos ao contratado dependerão dos quantitativos efetivamente fornecidos.

CLÁUSULA SEXTA - PAGAMENTO

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

CLÁUSULA SÉTIMA - REAJUSTE

- 7.1 Os preços inicialmente contratados são fixos e irreajustáveis no prazo de um ano contado da data do orçamento estimado, em ____/____/____ (DD/MM/AAAA).
- 7.2 Após o interregno de um ano, e independentemente de pedido do contratado, os preços iniciais serão reajustados, 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 Nos reajustes subsequentes ao primeiro, o interregno mínimo de um ano será contado a partir dos efeitos financeiros do último reajuste.
- 7.4 No caso de atraso ou não divulgação do(s) índice (s) de reajustamento, o contratante pagará ao contratado a importância calculada pela última variação conhecida, liquidando a diferença correspondente tão logo seja(m) divulgado(s) o(s) índice(s) definitivo(s).
- 7.5 Nas aferições finais, o(s) índice(s) utilizado(s) para reajuste será(ão), obrigatoriamente, o(s) definitivo(s).
- 7.6 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.
- 7.7 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.
- 7.8 O reajuste será realizado por apostilamento.

CLÁUSULA OITAVA - OBRIGAÇÕES DO CONTRATANTE

- 8.1 São obrigações do Contratante, além das previstas no Termo de referência:
- 8.2 Exigir o cumprimento de todas as obrigações assumidas pelo Contratado, de acordo com o contrato e seus anexos.
- 8.3 Receber o objeto no prazo e condições estabelecidas no Termo de Referência.
- 8.4 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.
- 8.5 Acompanhar e fiscalizar a execução do contrato e o cumprimento das obrigações pelo Contratado;
- 8.6 Comunicar a empresa para emissão de Nota Fiscal no que pertine à parcela incontroversa da execução do objeto, para efeito de liquidação e pagamento, quando houver controvérsia sobre a execução do objeto, quanto à dimensão, qualidade e quantidade, conforme o art. 143 da Lei nº 14.133, de 2021.
- 8.7 Efetuar o pagamento ao Contratado do valor correspondente ao fornecimento do objeto, no prazo, forma e condições estabelecidos no presente Contrato.
- 8.8 Aplicar ao Contratado as sanções previstas na lei e neste Contrato.
- 8.9 Não praticar atos de ingerência na administração do contratado, tais como (art. 48 da Lei n.º 14.133/2021):
- a) indicar pessoas expressamente nominadas para executar direta ou indiretamente o objeto contratado;
 - b) fixar salário inferior ao definido em lei ou em ato normativo a ser pago pelo contratado;
 - c) estabelecer vínculo de subordinação com funcionário do contratado;
 - d) definir forma de pagamento mediante exclusivo reembolso dos salários pagos;
 - e) demandar a funcionário do contratado a execução de tarefas fora do escopo do objeto da contratação;
 - f) prever exigências que constituam intervenção indevida da Administração na gestão interna do contratado.
- 8.10 Cientificar o órgão de representação judicial da Advocacia-Geral da União para adoção das medidas cabíveis quando do descumprimento de obrigações pelo Contratado.
- 8.11 Explicitamente emitir decisão sobre todas as solicitações e reclamações relacionadas à execução do presente Contrato, ressalvados os requerimentos manifestamente impertinentes, meramente protelatórios ou de nenhum interesse para a boa execução do ajuste.
- 8.11.1 A Administração terá o prazo de 30 dias, a contar da data do protocolo do requerimento para decidir, admitida a prorrogação motivada, por igual período.
- 8.12 Responder eventuais pedidos de reestabelecimento do equilíbrio econômico-financeiro feitos pelo contratado no prazo máximo de 30 dias.
- 8.13 Comunicar o Contratado na hipótese de posterior alteração do projeto pelo Contratante, no caso do art. 93, §2º, da Lei nº 14.133, de 2021.
- 8.14 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

- São obrigações da Contratada, além das previstas no Termo de referência:
- 9.1 A Contratada deve cumprir todas as obrigações constantes deste Contrato e de seus anexos, assumindo como exclusivamente seus os riscos e as despesas decorrentes da boa e perfeita execução do objeto, observando, ainda, as obrigações a seguir dispostas, além das previstas no termo de referência:
- 9.2 Manter preposto aceito pela Administração no local ou do serviço para representá-lo na execução do contrato.
- 9.2.1 A indicação ou a manutenção do preposto da empresa poderá ser recusada pelo órgão ou entidade, desde que devidamente justificada, devendo a empresa designar outro para o exercício da atividade.
- 9.3 Atender às determinações regulares emitidas pelo fiscal do contrato ou autoridade superior (art. 137, II) e prestar todo esclarecimento ou informação por eles solicitados.

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

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

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

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

9.8 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, até o dia trinta do mês seguinte ao da prestação dos serviços, os seguintes documentos:

a) prova de regularidade relativa à Seguridade Social;

b) certidão conjunta relativa aos tributos federais e à Dívida Ativa da União;

c) certidões que comprovem a regularidade perante a Fazenda Municipal ou Distrital do domicílio ou sede do contratado;

d) Certidão de Regularidade do FGTS – CRF; e

e) Certidão Negativa de Débitos Trabalhistas – CNDT;

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

9.10 Comunicar ao Fiscal do contrato, no prazo de 24 (vinte e quatro) horas, qualquer ocorrência anormal na prestação dos serviços.

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

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

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

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

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

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

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

9.18 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).

9.19 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).

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

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

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

CLÁUSULA DÉCIMA- 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.

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.

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

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

10.12 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

11.1 Não haverá exigência de garantia contratual da execução.

CLÁUSULA DÉCIMA SEGUNDA – INFRAÇÕES E SANÇÕES ADMINISTRATIVAS (da fase da execução contratual)

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;

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.

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” e “d” do subitem acima deste Contrato, sempre que não se justificar a imposição de penalidade mais grave (art. 156, § 4º, da Lei nº 14.133, de 2021);

iii. Declaração de inidoneidade para licitar e contratar, quando praticadas as condutas descritas nas alíneas “e”, “f”, “g” e “h” do subitem acima deste Contrato, bem como nas alíneas “b”, “c” e “d”, que justifiquem a imposição de penalidade mais grave (art. 156, §5º, da Lei nº 14.133, de 2021).

iv. Multa, considerando os parâmetros descritos no termo de referência:

Falha apurada	Fundamento legal	Sanção	Multa
Dar causa à inexecução parcial do contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho
Deixar de prestar garantia ou assistência técnica aos materiais fornecidos	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho
Recusar-se ou deixar de prestar parcela do Contrato de fornecimento ou de prestação dos serviços, nos prazos contratados	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho
Interromper a prestação dos serviços ou o fornecimento continuado, após iniciada a execução do Contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	Até 10% do valor total remanescente da obrigação
Recusar-se ou deixar de atender solicitação formal da fiscalização do Contrato, necessários à boa execução contratual	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho
Recusar-se ou deixar de cumprir normas internas da UFPR, apontadas em relatório de fiscalização	Lei 14.133/2021, art. 155 inc. I	Advertência	De 6 a 20% do valor do empenho

Deixar de ressarcir danos ao patrimônio da UFPR ou à integridade física ou patrimonial de terceiros, em decorrência de ação ou omissão durante a execução do Contrato	Lei 14.133/2021, art. 155 inc. I	Advertência	Moratória de 0,2% por dia em que a falha persistir. Compensatória de até 10% do valor do empenho, sem prejuízo das demais custas com o ressarcimento dos danos causados
Entregar material ou serviço com características diversas daquelas constantes no Edital de Licitação, recusando-se ou deixando de efetuar a substituição no prazo fixado pela UFPR	Lei 14.133/2021, art. 155 inc. I	Advertência	Até 10% em relação ao valor da obrigação
Entregar material ou serviço com características diversas daquelas constantes no Edital de Licitação, efetuando a substituição fora do prazo fixado pela UFPR	Lei 14.133/2021, art. 155 inc. I	Advertência	Moratória de 0,5% por dia de atraso Compensatória de até 5% em relação ao valor da obrigação
Dar causa à inexecução parcial do contrato que cause grave dano à Administração ou ao funcionamento dos serviços públicos ou ao interesse coletivo	Lei 14.133/2021, art. 155 inc. II	Impedimento de licitar e contratar no âmbito da União por até 1 ano	Agravada em 50% em relação à prevista para os casos de advertência
Dar causa à inexecução total do contrato	Lei 14.133/2021, art. 155 inc. III	Impedimento de licitar e contratar no âmbito da União por até 3 anos	Até 30% em relação ao valor total do Contrato
Recusar-se ou deixar de fornecer os materiais ou de prestar os serviços, integralmente	Lei 14.133/2021, art. 155 inc. III	Impedimento de licitar e contratar no âmbito da União por até 3 anos	Até 30% em relação ao valor total do Contrato
Ensejar o retardamento da execução ou da entrega do objeto da contratação sem motivo justificado	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Até 10% em relação ao valor total do Contrato
Atrasar a entrega de material ou serviço por prazo de até 30 dias	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Moratória de 0,3% por dia de atraso
Atrasar a entrega de material ou serviço por prazo superior a 30 (trinta) dias	Lei 14.133/2021, art. 155 inc. VII	Impedimento de licitar e contratar no âmbito da União por até 2 anos	Moratória de 0,5% por dia de atraso Compensatória de até 5% em relação ao valor da obrigação
Prestar declaração falsa durante a execução do contrato	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato

Fazer declaração falsa sobre seu enquadramento fiscal	Lei 14.133/2021, art. 155 inc. VIII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
Praticar ato fraudulento na execução do contrato	Lei 14.133/2021, art. 155 inc. IX	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
Comportar-se de modo inidôneo	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
Cometer fraude de qualquer natureza	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
Omitir informações em notas fiscais	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
Falsificar ou alterar notas fiscais	Lei 14.133/2021, art. 155 inc. X	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato

Praticar ato lesivo previsto no art. 5º da Lei nº 12.846, de 1º de agosto de 2013	Lei 14.133/2021, art. 155 inc. XII	Declaração de inidoneidade para licitar e contratar no âmbito da Administração Pública direta e indireta de todos os entes federativos, pelo prazo de 36 a 60 meses	Até 30% do valor total do Contrato
---	------------------------------------	---	------------------------------------

***6% de 1/12 = 0,5% do valor total do contrato

12.2.1. As sanções listadas na tabela acima não esgotam a possibilidade de enquadramento das condutas da Contratada nas infrações previstas nesta Seção, com a aplicação das penalidades cabíveis.

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).

12.4.1 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)

12.4.2 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).

12.4.3 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 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.

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 TERCEIRA– DA EXTINÇÃO CONTRATUAL

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

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

13.3 A extinção nesta hipótese ocorrerá na próxima data de aniversário do contrato, desde que haja a notificação do contratado pelo contratante nesse sentido com pelo menos 2 (dois) meses de antecedência desse dia.

13.4 Caso a notificação da não-continuidade do contrato de que trata este subitem ocorra com menos de 2 (dois) meses da data de aniversário, a extinção contratual ocorrerá após 2 (dois) meses da data da comunicação.

13.5 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.

13.5.1 Nesta hipótese, aplicam-se também os artigos 138 e 139 da mesma Lei.

13.5.2 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.

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

13.6 O termo de extinção, sempre que possível, será precedido:

13.6.1 Balanço dos eventos contratuais já cumpridos ou parcialmente cumpridos;

13.6.2 Relação dos pagamentos já efetuados e ainda devidos;

13.6.3 Indenizações e multas.

13.7 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).

13.8 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).

CLÁUSULA DÉCIMA QUARTA – DOTAÇÃO ORÇAMENTÁRIA

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: Pró-Reitoria de Administração;

II) Fonte de Recursos:

III) Programa de Trabalho:

IV) Elemento de Despesa:

V) Plano Interno:

VI) Nota de Empenho: XXXXXXXXXX

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

CLÁUSULA DÉCIMA QUINTA – DOS CASOS OMISSOS

15.1 Os casos omissos serão decididos pelo contratante, segundo as disposições contidas na Lei n.º 14.133, de 2021, e demais normas federais aplicáveis e, subsidiariamente, segundo as disposições contidas na Lei n.º 8.078, de 1990 – Código de Defesa do Consumidor – e normas e princípios gerais dos contratos.

CLÁUSULA DÉCIMA SEXTA – ALTERAÇÕES

16.1 Eventuais alterações contratuais reger-se-ão pela disciplina dos arts. 124 e seguintes da Lei n.º 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 n.º 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 n.º 14.133, de 2021.

CLÁUSULA DÉCIMA SÉTIMA – 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 n.º 14.133, de 2021, e art. 8º, §2º, da Lei n.º 12.527, de 2011, c/c art. 7º, §3º, inciso V, do Decreto n.º 7.724, de 2012.

CLÁUSULA DÉCIMA OITAVA – FORO

18.1 Fica eleito o Foro da Justiça Federal - Seção Judiciária do Paraná / Subseção Judiciária de Curitiba 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 n.º 14.133/21.

[Local], [dia] de [mês] de [ano].

Representante legal do CONTRATANTE

Representante legal do CONTRATADO

TESTEMUNHAS:

1-

2-